Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's *1984* to Life and What the Law Should Do About It

Jill Yung[*]

[*] Law clerk to Judge William Shubb, Eastern District of California (2005–06). J.D., Northwestern University School of Law. For invaluable comments, discussions, and encouragement, thanks to Sue Provenzano, who also suggested this topic. Thanks also to the editors of the *Seton Hall Law Review* for their terrific work on this piece.

I. INTRODUCTION

> The telescreen received and transmitted simultaneously. Any sound that [a person] made, above the level of a very low whisper, would be picked up by it. . . . There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual was guesswork. It was even conceivable that they watched everybody all the time. . . . You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and . . . every movement scrutinized.[1]

Nineteen eighty-four came and went without realizing the bleak existence imagined in George Orwell's novel, set in a world where the terms "privacy" and "freedom" were, literally, scheduled to be erased from the common vernacular.[2] However, a survey of modern technology and its uses just twenty years later raises the question: was Orwell altogether wrong, or just overzealous in his estimates of how long it would take to erode completely our understanding of

---

[1] GEORGE ORWELL, 1984, at 4 (1949).

[2] *Id.* at 53 (describing the work of those compiling the "Eleventh Edition of the Newspeak dictionary" and the ultimate goal: to make "[e]very year fewer and fewer words, and the range of consciousness always a little smaller" until "[e]very concept that can ever be needed will be expressed by exactly *one* word"); *see also id.* at 54 (speaking optimistically of a time "when the concept of freedom has been abolished").

personal space and privacy? In the context of employment, an Orwellian reality is not as fanciful as once thought, for new developments in employee surveillance programs threaten to bring us closer to the world Orwell envisioned.[3] With the advent of Global Positioning System ("GPS") tracking services, employers can now purchase technology that allows them to *watch everybody all the time* and *scrutinize every movement.*

Other commentators have already expressed concern about various types of employee surveillance. The alarm bells went off when video surveillance and Internet tracking software debuted in workplaces.[4] Still, these practices, limited somewhat by a need to show business-relatedness, have largely found acceptance in some form.[5] GPS monitoring programs, however, raise unique issues that arguably go beyond acceptable boundaries for employee surveillance. Because GPS tracking systems can, have, and likely will continue to capture off-duty movements of employees,[6] this form of surveillance is more nefarious than the types of employee monitoring programs debated elsewhere.

Moreover, in contrast to the at-work monitoring of, for example, e-mail and Internet use, the after-hours stalking of employees bears no relationship to productivity, trade secret theft, or harassment prevention efforts—a few of the reasons employers have proffered to justify monitoring activities in other contexts.[7] GPS is a prime example of "technology [that enables] employers to gather enormous amounts of data about employees, *often far beyond what is necessary to satisfy safety or productivity concerns.*"[8] Even more disconcerting, "the

---

[3] *See* Eric Wieffering, *Blurring of Home, Online and Work May Redraw Privacy Limits*, MINNEAPOLIS STAR TRIB., Feb. 13, 2000, at A1 ("'We used to worry that Big Brother would be the government,' said Craig Cornish, a Colorado attorney who specializes in worker privacy rights. 'But Big Brother is increasingly the employer.'").

[4] *See, e.g.*, Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289 (2002) (electronic monitoring of Internet use); Stephen B. Stern & Pamela J. White, *Legal Risks of Electronic Surveillance in the Workplace*, MD. B. ASS'N, Jan.–Feb. 2002, at 3 (video surveillance).

[5] Kristen Bell DeTienne & Richard D. Flint, *The Boss's Eyes and Ears: A Case Study of Electronic Employee Monitoring and the Privacy for Consumers and Workers Act*, 12 LAB. LAW. 93, 93 (1996) ("Traditionally, employers in America have been allowed to eavesdrop, videotape, tap phone lines, and search through computer files, without employee knowledge or consent. In fact, some federal laws that prohibit wire tapping and other forms of spying specifically exempt employers . . . .").

[6] *See* discussion *infra* Part II.D.

[7] Tonianne Florentino, *Privacy in the Workplace*, 788 PLI/PAT. 551, 563 (2004).

[8] FREDERICK S. LANE III, THE NAKED EMPLOYEE: HOW TECHNOLOGY IS COMPROMISING WORKPLACE PRIVACY 3–4 (2003) (emphasis added).

trends that drive technology—faster, smaller, cheaper—[will] make it possible for larger and larger numbers of employers to gather ever-greater amounts of personal data"[9] by saddling their employees with GPS tracking devices.

Location determination technologies have proliferated rapidly in the workplace not only because of technology's seemingly instinctive ability to develop faster than the laws that might control it,[10] but also because federal regulations have lowered the cost of utilizing these services. The Federal Communications Commission ("FCC") imposed a December 31, 2002 deadline on mobile phone service providers to update their product lines to include only phones capable of pinpointing a user's location.[11] This translated to a requirement that new phones function as GPS receivers. Additionally, the regulations tasked service providers with the chore of ensuring that ninety-five percent of their customers possess "location-capable" phones by December 31, 2005—a deadline that is rapidly approaching.[12] Through this regulation, the FCC hopes to provide faster and more accurate emergency service to those who make 9-1-1 calls from cell phones.[13] But with nearly every cell phone owner toting a GPS tracking device in their pocket or purse, this development also has unintentional benefits for the emerging personnel and fleet management industry.[14] Soon, companies will be able to *stalk* the large number of people in their workforce who carry cell phones.

Without reasonable statutory restrictions on employee tracking techniques, workers will need to rely on existing laws and doctrines, which this Article will expose as wholly inadequate to handle this emerging problem.[15] Defenseless, employees thus face the danger

---

[9] *Id.*; *see also* Otis B. Grant, *Law and Perceptions: Internal Investigations and Employee Privacy Interests in Public Sector Employment*, 71 UMKC L. REV. 1, 24 (2002) (warning that "[w]ith the advent of new technology, employee monitoring will steadily increase as it becomes cheaper to perform").

[10] William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOK. L. REV. 91, 103 (2003) (characterizing "electronic monitoring [as] an area where technology has outstripped the law, leaving employees largely unprotected").

[11] 47 C.F.R. § 20.18(g)(1)(iv) (2004).

[12] *Id.* § 20.18(g)(1)(v).

[13] *Id.* § 20.18 (establishing the E-911 program); *see also* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 381 (2003).

[14] One author described the E-911 program as "[p]erhaps the single most important thrust area for locator services." John A. Lever, *Unintended Consequences of the Global Positioning System*, SYSTEMS ENGINEERING, May 6, 2004, at 217, *available at* http://www3.interscience.wiley.com/cgi-bin/abstract/108563806/ABSTRACT.

[15] *See* discussion *infra* Part III.

that electronic devices will erode their personal privacy,[16] a fear first articulated by Samuel D. Warren and Louis D. Brandeis in their seminal work, *The Right to Privacy*.[17] Once again, "[t]he intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world . . . ."[18] Without some form of legal protection for off-duty employees, however, employers will have an unchecked ability to follow them into that retreat,[19] making note of every place an employee stops along the way.

On the other side of the debate, GPS monitoring certainly offers attractive benefits for employers. These devices enable companies to provide faster service and increase productivity through better coordination of employees who work remotely—particularly advantageous features for employers of delivery and maintenance workers.[20] They also function as risk management tools by facilitating faster recovery of stolen property and encouraging respect for traffic rules.[21] But when the workday ends, many of the justifications for monitoring become irrelevant.[22]

Additionally, these interests should be weighed against the negative impact that employee surveillance tends to have on its subjects. Monitoring "takes its toll on workers and companies in terms of stress, fatigue, apprehension, motivation, morale, and trust; this results in increased absenteeism, turnover, poorer management,

---

[16] Peter J. Isajiw, Comment, *Workplace Email Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 TEMP. ENVTL. L. & TECH. J. 73, 74 (2001).

[17] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[18] *Id.* at 196 (discussing how the press was, at the time "overstepping in every direction the obvious bounds of propriety and of decency").

[19] The technology "rarely works anywhere but outdoors." David A. Schumann, *Tracking Evidence with GPS Technology*, WIS. LAW., May 2004, at 62 n.13. But given how far the technology has come, this obstacle will likely be overcome in the near future. Some reports claim that companies, including Sprint, already have technology that "can pinpoint a phone's location within . . . 1,000 feet if it is inside." David Hayes, *Locator Phones: Spies or Helpers?*, KAN. CITY STAR, May 16, 2005, at A1.

[20] *See* DeTienne & Flint, *supra* note 5, at 95–96; *see also infra* note 56 and accompanying text.

[21] *See* discussion *infra* notes 60–61, 65 and accompanying text.

[22] Granted, regardless of whether an employee is off-duty, other employer interests may be furthered by after-hours monitoring when company vehicles, vulnerable to theft or misuse, are involved. However, these concerns are not relevant for every employer using GPS tracking devices and exceptions, like the one described in the statutory proposal in Part V.C.3 of this Article, can protect legitimate after-hours interests in valuable employer-owned property.

and lower productivity, not to mention higher health-care costs."[23] By failing to legislate in this area and allowing employers to exercise an absolute power to stalk employees around the clock, government implicitly favors the employers' interests over those of employees, who have an equally substantial stake in how the law approaches this issue. For example:

> [E]mployment is a key source of self-esteem for many workers. Individuals often define themselves by their occupations, which becomes a significant aspect of their personae. Because of the substantial interests individuals have in both employment and in privacy, invasive monitoring puts employees in a "catch-22" situation, forcing them to sacrifice reasonable expectations of privacy because of their need to work.[24]

The law should not enable employers to put employees in this impossible position.

After-hours GPS monitoring takes two controversial issues in employment law—electronic monitoring and discipline for off-duty activity—and combines them, creating the potential for a "worst of both worlds" situation. Legislators and courts have found reasonable exceptions that separately allow for electronic monitoring in the workplace and off-duty observations in some contexts,[25] but off-duty GPS tracking of employees goes beyond these tolerable limits.

Motivated by these concerns, this Article will attempt to build a case for why and how off-duty GPS tracking of employees should be limited by federal statute. Part II provides historical information regarding the development of GPS technology, how it became a part of civilian business operations, and its impact on workers thus far. Part III explores the potential legal theories that might provide a means for balancing employer interests in using technology that enhances efficiency and employee interests in maintaining some shred of privacy in a world where personal lives are increasingly less

---

[23] Kesan, *supra* note 4, at 320; *see also* 139 CONG. REC. S6122, 6123 (1993) (statement of Sen. Paul Simon in support of S. 984) (recalling the testimony of a Northwest Airlines sales representative who was electronically monitored so pervasively "that she had to get a doctor's note to limit the amount of monitoring she [was] to be subjected to during a work day due to the stress and health problems the monitoring had caused"). Given these effects, one would think that employers would recognize on their own how short-sighted the ruthless operation of an electronic sweatshop really is; but even economic losses resulting from employee stress have not dampened employers' interest in gathering more information about their employees.

[24] S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 835 (1998).

[25] *See* discussion *infra* Part III.B.2 and *infra* notes 144–45 and accompanying text.

distinguishable from work lives.[26] This section concludes, however, that existing legal doctrines are imperfect vehicles for the pursuit of an employee's right not to be monitored after hours. Part IV explores how the law has responded to the use of GPS devices to monitor people in other contexts and observes that, in an unregulated world, the rights of employees most closely resemble those of suspected and convicted criminals, when they should instead correspond with the rights against surreptitious monitoring that state legislators have recently created for consumers. Part V thus seeks to develop an acceptable proposal for a federal law governing after-hours monitoring of employees. This section explores recent failed efforts to create generic employee privacy laws and attempts to remedy the shortcomings of these bills by proposing a more narrow solution targeted at one of the more egregious forms of employee privacy violations: the constant surveillance of the off-duty activities of employees.

II. TECHNOLOGY BACKGROUND

As with other technological developments, GPS tracking systems threaten to outpace lawmakers' abilities to ensure that old rights are not sacrificed in exchange for the "convenience" offered by modern machinery.[27] Blinded by the glowing screen of each new gadget, society generally tends to moon over efficiency gains without considering the true cost of living in a more automated society. The story behind the evolution of GPS monitoring technology reveals another invention falling into this pattern, in which the modern marvel becomes, under some circumstances, the modern menace.

---

[26] Wieffering, *supra* note 3.

[27] *See* LANE, *supra* note 8, at 185 (discussing the "persistent tension between 'privacy'—our innate desire to control the information that is known about us—and 'convenience'—our equally innate desire for day-to-day life to be a little easier"). Lane offers Internet technologies, capable of remembering preferences and payment information, as one example of the trade-off between privacy and convenience. *Id.* The same technology that relieves us of having to retype personal information for every Internet transaction also "help[s] websites track which pages we look at and the sites we visit afterwards." *Id.* Going back even further, Lane reminds us that we also traded huge amounts of information about our shopping, eating, and travel habits to credit card companies in exchange for the convenience of not having to carry cash. *Id.* "The trading of privacy for convenience has become so commonplace that we often don't even think about it." *Id.*

A. GPS Technology and How It Works

From the beginning, the Global Positioning System was designed to track an increasingly mobile population, although not the civilian masses who are now the targets of its unblinking gaze.[28] The military developed the technology after the Vietnam War "to form a worldwide navigational system"[29] that could track troops on the ground in remote locations.[30] The resulting GPS infrastructure consisted of twenty-four primary satellites, arranged in six orbital planes, and a handful of spares[31] that now circle the earth every twelve hours from a distance of about 10,900 nautical miles.[32] At any given time, five satellites are visible from a given point on earth, although determining a receiver's location requires using only three to four satellites.[33] By measuring the length of radio signals emitted by these satellites, a receiver on earth can calculate its own location, within ten to 100 meters, by "triangulating" the signals.[34] Additionally, "[i]f a person is mobile, a GPS receiver may calculate the person's speed and direction of travel . . . ."[35]

---

[28] One author has described GPS as "an asset of the U.S. Government that has seen widespread adoption in the last decade, far beyond its original intended purpose." Lever, *supra* note 14, at 220.

[29] RICHARD RAYSMAN ET AL., EMERGING TECHNOLOGY: FORMS & ANALYSIS § 1.03 (2003).

[30] Richard C. Balough, *Global Positioning System and the Internet: A Combination with Privacy Risks*, 15 CBA REC. 28, 29 (Oct. 2001).

[31] The number of spares appears to fluctuate. At the start of 2003, with only two back-ups in place, the United States launched its first new addition since 2001. Justin Ray, *Delta Rocket Launches GPS Navigation Satellite*, SPACEFLIGHT NOW, Jan. 29, 2003, http://spaceflightnow.com/delta/d295 [hereinafter Ray, *Delta Rocket Launches*]. Subsequently, hurricanes and other weather-related obstacles interfered with launches in 2004. *Worldwide Launch Schedule*, SPACEFLIGHT NOW, http://spaceflightnow.com/tracking (last visited Sept. 25, 2005). At last count, the military had a total of twenty-eight craft (twenty-four functioning satellites and four back-ups), in place for navigation purposes. Justin Ray, *Delta Rocket Successfully Launches One for The Gipper*, SPACEFLIGHT NOW, June 23, 2004, http://www.spaceflightnow.com/delta/d305.

[32] Balough, *supra* note 30, at 29; Ray, *Delta Rocket Launches*, *supra* note 31.

[33] SCOTT PACE ET AL., THE GLOBAL POSITIONING SYSTEM: ASSESSING NATIONAL POLICIES app. A, at 218 (1995), *available at* http://www.rand.org/publications/MR/MR614/MR614.appa.pdf.

[34] Balough, *supra* note 30, at 29; *see also* David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 4 (2003) (explaining that "[t]riangulation calculates the user's location by comparing the same signal as it arrives at several receiving towers"). Depending on the number of satellites involved in the calculation, a GPS receiver may be able to determine its altitude in addition to its geographic position. RICHARD RAYSMAN ET AL., *supra* note 29.

[35] RAYSMAN ET AL., *supra* note 29.

In 1983, after the Russians shot down a disoriented Korean Airlines flight that mistakenly entered Russian airspace, President Ronald Reagan approved the commercial use of the military's GPS infrastructure.[36] At first, civilian use of the technology developed slowly in niche markets such as surveying and aviation.[37] Then, just as the 24-satellite constellation in place today neared completion, "[t]he success of GPS in Operation Desert Storm sparked a surge in a growing multi-million-dollar market that had barely existed just a few years prior to the war."[38] News coverage of "soldiers navigat[ing] across a featureless desert" and "bomber units target[ing] the enemy with unprecedented accuracy" essentially provided free advertising for GPS service providers.[39]

The industry grew rapidly after these events and continues to expand. "[S]ome analysts now predict that the burgeoning industry may see annual revenues as high as $34 to $41 billion by 2006."[40] Additionally, the product line continues to diversify and currently includes services ranging from OnStar's Neverlost system, an onboard navigation tool that guides drivers to a user-specified destination, to Wherify and Digital Angel's personal tracking wristwatches, ideal devices to use when pursuing a kidnapped toddler or rebellious teenager.[41] Despite the ever-expanding array of available services,

---

[36] Waseem Karim, Note, *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring*, 14 WASH. U. J.L. & POL'Y 485, 485 & n.3 (2004) (citing ALESSANDRA A.L. ANDRADE, THE GLOBAL NAVIGATION SATELLITE SYSTEM: NAVIGATING INTO THE NEW MILLENNIUM 37, 38, 53 n.6 (2001)).

[37] PACE ET AL., *supra* note 33, app. B, at 248–49.

[38] *Id.* at 250. Shortages of military receivers further stimulated sales of civilian GPS products as the military had to purchase thousands of privately manufactured devices for its operations in Iraq. To use these devices, the military also had to make the system more accessible to civilian products, which enhanced the accuracy of commercial GPS receivers. *Id.* at 250–51.

[39] *Id.*

[40] LANE, *supra* note 8, at 200; *see also* James C. White, People, Not Places: A Policy Framework for Analyzing Location Privacy Issues 13 (Spring 2003) (unpublished M.A. memorandum, Duke University), http://www.epic.org/privacy/location/jwhite locationprivacy.pdf ("[B]y 2006, the worldwide market for location-based services is expected to be almost $40 Billion."). *Contra Employee Tracking Technology Raises Concerns About Privacy*, 174 Lab. Rel. Rep. (BNA) 347 (May 10, 2004) (offering a more conservative estimate, predicting that "[l]ocation-based services—which can be used to monitor employee movement—will be a $15 billion industry by 2007 as a variety of interested companies scramble to implement it in various elements of their business operations" (quoting Cindy-Ann L. Thomas, Taft HR Solutions)).

[41] Karim, *supra* note 36, at 488–92 (describing personal tracking devices). The industry's plans are not, however, limited to stand-alone tracking devices. Firms like Applied Digital Solutions, the maker of VeriChip, have designed more invasive devices that are "surgically imbedded underneath a person's skin," *id.* at 490–92,

however, this Article focuses exclusively on one segment of the market: the fleet and personnel management tools that, unbeknownst to many employees, are already in place, monitoring a worker's every move. The next section describes these tools and services and the companies that deploy them.

B. Packages Offered for Employee Monitoring and the Companies That Use Them

As previously noted, employers do have compelling reasons for using GPS tracking systems to monitor a mobile workforce.[42] Many fleet management programs tout their ability to prevent theft of company assets, verify employee productivity, and reduce insurance premiums by providing carriers with evidence that drivers comply with traffic laws. These companies offer a variety of tracking options, ranging from "active" systems that report location data at regular intervals, to "passive" devices that log downloadable tracking information. Thus, when choosing a system, employers must weigh their interests in having such services and business needs against cost and system complexity.[43] The following provides a sampling of the specific services these tracking companies offer.

One example of a workforce monitoring program is Aligo's WorkTrack, an active, real-time system that allows employers to monitor time and location information via the Internet.[44] Like many systems, Aligo promotes itself as "an easy, accurate way to manage the time of your mobile employees, raising productivity and bringing

---

causing some to speculate "that it is only a matter of time until people are routinely 'scanned like a box of Wheaties.'" Marren Sanders, *Chipping: Could a High Tech Dog Tag Find Future American MIAs?*, 4 J. HIGH TECH. L. 209, 211 (2002) (citation omitted). Indeed, the FDA's recent approval of VeriChip implants moved the United States one step closer to this reality. *FDA OKS Implanted Medical Info Chip*, CNN, Oct. 13, 2004, http://www.cnn.com/2004/HEALTH/10/13/fda.implant.chip.ap/index.html. *But cf.* Barnaby J. Feder & Tom Zeller, Jr., *Identity Chip Planted Under Skin Approved for Use in Health Care*, N.Y. TIMES, Oct. 14, 2004, at A1 (reporting that although Applied Digital Solutions hopes that the VeriChip's approved medical use will "accelerate the acceptance of under-the-skin ID chips as security and access-control devices," the chips do not currently have "the ability to track individuals via satellite").

[42] *See supra* notes 20–22 and accompanying text.

[43] ERETAILNEWS, ERETAILREPORT: GLOBAL POSITIONING SYSTEMS FOR RETAIL FLEET MANAGEMENT 6 (2001), http://www.eretailnews.com/issues/2001-7.PDF. Hybrid active/passive systems are also available, as well as systems that use another set of satellites for two-way communication. *Id.* at 3.

[44] Aligo – The Mobile Enterprise Software Company, WorkTrack, http://www.aligo.com/products/workTrack (last visited Sept. 25, 2005).

substantial cost savings to your business."[45] However, unlike other products that merely track movements of an employer's equipment, such as a company car, Aligo monitors employees using "the GPS-enabled phones they already carry . . . ."[46]

This technology is troublesome for two reasons. First, cell phone tracking systems, based on hand held devices, allow employers to monitor not only their equipment, but, more specifically, the people who carry it. Although Aligo has an "on break" mode, the marketing materials suggest that this feature exists for the employer's benefit, not the employee's. This function allows the employer to record time more accurately—the materials say nothing about whether the employee can use this feature to prevent his employer from hunting him down when he is "on break," or even off the job entirely, if the device is turned off.[47] Devices that continue to relay location information after an employee clocks out give employers control, or at least influence, over an employee's uncompensated time and invite overbearing invasions of privacy. Second, assuming that the device can be tracked after-hours and while off, an employer might discipline an employee for someone else's extracurricular activity. No feature offers confirmation that the device remained in the employee's possession at all times.

The system offered by Comet Tracker is only slightly less invasive. As a phone-based system, it has the potential, like Aligo's WorkTrack, to mistakenly attribute the location of a misplaced phone to the employee responsible for it. The system does, however, have

---

[45] *Id.*

[46] *Id.*

[47] *Id.* Given that the devices can be used to "[a]lert[] the central office of status and availability to take new jobs" and "[d]isplay[] a current map with the location of your entire workforce," the technology appears to track workers both on and off the job. *Id.* Even more disconcerting for the employees, Aligo promises "continuous access, regardless of connectivity." *Id.* This statement seems to give more credence to the assumption that the products can function as homing devices even when turned off. *See also* NAT'L WORKRIGHTS INST., ON YOUR TRACKS: GPS TRACKING IN THE WORKPLACE 11 (2004), http://www.workrights.org/issue_electronic/NWI_GPS_Report.pdf ("[I]n some cases, even when the devices appear to be turned off, they still emit detectable signals."); Stacy A. Teicher, *It's 2 a.m. Do You Know Where Your Workers Are?*, CHRISTIAN SCI. MONITOR, Dec. 22, 2003, *available at* http://www.csmonitor.com/2003/1222/p14s02-wmgn.html (speaking generally of GPS tracking devices embedded in cell phones and noting that "[i]n some cases, even when the devices appear to be turned off, they still emit signals that can be detected"). Perhaps most frightening, however, is Aligo's promise to enable employers to "*[a]lways know* where [their] employees are." Aligo – The Mobile Enterprise Software Company, WorkTrack, http://www.aligo.com/products/workTrack (emphasis added) (last visited Sept. 26, 2005).

an automatic shut off feature that prevents after-hours tracking.[48] In exchange for this "protection" though,[49] employees monitored using Comet Tracker must operate within a "geofence"—a predefined area that, when breached, will trigger an alert.[50] Again, this technology puts the worker who takes an innocent detour to avoid traffic or road construction at an incredible disadvantage as he or she might be fired for venturing out of the employer's virtual cage.[51] Employers may be interested in "always know[ing] exactly where [their] workers are—and where they've been,"[52] but do they really *need* such far-reaching power over their employees—especially after-hours?

Employees might feel slightly less threatened by FleetBoss Global Positioning Solutions' fleet management services. Using GPS tracking devices, FleetBoss monitors vehicles, not people, although this might be of little consequence to the employee who stops to run an errand on the way home in the company car and unintentionally reveals information about her personal life to her employer. FleetBoss might discourage employees from "going home, . . . to Wal-Mart and [to] the grocery store on company time,"[53] but what happens when an employer virtually observes the employee stopping during her lunch hour at Planned Parenthood and fires her based on

---

[48] Comet Tracker Overview, *available at* http://www.comettracker.com/overview.html (describing the features of Comet Tracker, the company's brochure claims to offer employers the ability to "[a]lert workers to start tracking" and "[a]utomatically *stop tracking* at the end of the day" (emphasis added)). Although the program appears to place all control over the timing and duration of monitoring in the hands of the employer, at least the system offers a technically feasible cloaking capability.

[49] The Author remains skeptical that the physical ability to turn off the phone can offer employees much relief given that the employer is likely to assume the worst if an employee decides to shield her activities from observation. *See* LANE, *supra* note 8, at 207 ("If a constant stream of location data is the norm in your workplace, then information gaps are going to be suspicious. Sometimes, the absence of data can be just as problematic as reams of it.").

[50] Comet Tracker, *available at* http://www.actsoft.com/products/tracker.html (describing communication features capable of "[a]utomati[cally] email[ing] an alert when workers . . . travel outside their set home areas").

[51] *See* Ben Charny, *Big Boss Is Watching*, C|NET NEWS.COM, Sept. 24, 2004, http://news.com.com/Big+boss+is+watching/2100-1036_3-5379953.html (describing Xora's "'geofences' technology that sets off an alarm at the office when field workers go to preprogrammed off-limits sites, such as a bar or a park"); Charny, *supra* ("'There's no electro shock—yet,' Xora CEO Sanjay Shirole said.").

[52] Comet Tracker, How Do You Track Your Workers? (2003), http://www.comettracker.com/nextel/docs/CometTrackerFlyer.pdf.

[53] FleetBoss Global Positioning Solutions, Fleet Management – Business Needs Survey, http://www.fleetboss.com/needssurvey.asp (follow "Overtime Tip" hyperlink) (last visited Sept. 26, 2005) (quoting ServiceMaster, Lakeland, FL, a satisfied FleetBoss customer).

assumptions about her position on family planning methods?[54] Even programs that only monitor vehicles can threaten to restrict the activities of mobile employees while they are on breaks or off-duty and not being compensated by their employer. In fact, after-hours control over workers in part motivated at least one FleetBoss customer, Mr. Rooter Plumbing, to subscribe to FleetBoss' services.[55]

This discussion describes just a few of the many service providers clamoring for a piece of this emerging market. Employers already using these services include Orkin Pest Control (FleetBoss), Sun Microsystems (WorkTrack), and Lucent Technologies (WorkTrack).[56] Customers are often companies that, like those mentioned, have a deployable service-providing workforce. The tracking services, however, might appeal to any employer that desires more control over the productivity of largely unsupervised employees. Corporate lawyers, already equipped with the industry's standard issue BlackBerry, might some day find themselves subject to similar tracking programs.[57]

C. The Business Case for Using GPS to Monitor Employees and Equipment

Although the discussion in Part II.B described GPS monitoring systems as somewhat sinister and suspect, a fair discussion of these programs must recognize the legitimate business objectives achieved using monitoring services. Generally, an employer's interest in tracking its mobile workforce will stem from either an interest in

---

[54] LANE, *supra* note 8, at 200 ("What if you stop at Planned Parenthood on your lunch break and your supervisor wants to know if you're pregnant?").

[55] FleetBoss Global Positioning Solutions, Fleet Management Testimonials: Rob Birnie of Mr. Rooter Plumbing, http://www.fleetboss.com/testimonials.asp?REFERENCE_ID=53 (last visited Sept. 26, 2005) (describing one customer's requirements: "Drivers take trucks home, so after hours monitoring was needed").

[56] FleetBoss Global Positioning Solutions, Fleet Management Testimonials, http://www.fleetboss.com/testimonials.asp (last visited Sept. 26, 2005); Aligo Inc., Aligo Customers, http://www.aligo.com/customers/ (last visited Sept. 26, 2005). Comet Tracker does not provide a list of customers.

[57] Research In Motion's ("RIM") BlackBerry is a wireless e-mail device, phone, and electronic organizer all rolled into one. The company claims that over eighty percent of AmLaw 200 firms use its products to make the lives of mobile attorneys more manageable. BlackBerry.com, *BlackBerry for the Legal Community*, http://www.blackberry.com/solutions/industry/legal/index.shtml?CPID=ILC-hllegal (last visited Sept. 26, 2005). But the reverse may also be true—equipped with a GPS receiver in accordance with new FCC regulations, *see supra* notes 11–13 and accompanying text, the BlackBerry could be used to manage the attorneys themselves, not just their schedules. The invasion of privacy may be staged by employers of every stripe—not just those who manage delivery services.

limiting employer liability or in maintaining effective business operations (or both).[58] This section will explain each of these categories in turn.

First, concern about liability for employee torts and work-related injuries can justify an employer's interest in monitoring how employees perform away from the office. "If employees were solely responsible for their own actions, the need for surveillance would be greatly reduced . . . . [But] the doctrine of respondeat superior—which provides that an employer is liable for the negligence of an employee—has become an integral part of our legal system."[59] As the GPS service providers point out, the ability to monitor and discipline employees for speeding can significantly reduce employer liability for accidents and other traffic violations.[60] Moreover, "[i]nsurers will likely reward employers that monitor employees with lower rates, because GPS information will help predict and control risk, and confirm legitimate claims for early payment," thus providing employers with still more incentives to monitor speed.[61] Finally, in the event that a worker is injured in the field, the ability to quickly pinpoint his location and provide medical assistance may reduce the extent of his injuries and resulting workers' compensation costs.[62] Employers do not enjoy less responsibility for providing a safe

---

[58] Marisa Anne Pagnattaro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L. 625, 628 (2004).

[59] LANE, *supra* note 8, at 187. Lane explains that "[t]he theory behind the doctrine is that employers have the ability to control the actions of their employees, through both training and company policy, and therefore are liable for the injuries that their employees cause within the scope of their duties." *Id.* But Lane also notes, perhaps cynically, that "[t]he practical motivation is that the employer generally has greater resources (or can afford more insurance) and is therefore in a better position to compensate the injured party." *Id.*

[60] *See* Xora, *Industry Solutions Brief: Transportation & Distribution*, http://www.xora.com/timetrack/documents/pdf/LQ/Industry_Solutions_Transportation.pdf (monitoring an employee's speed "helps to ensure the safety of a company's driver staff as well as other motorists, while protecting the customers' shipments").

[61] Schumann, *supra* note 19, at 61; Xora, *supra* note 60 (promoting Xora's GPS TimeTrack product by claiming that "if the drivers have better driving records, companies can keep insurance costs down").

[62] Kesan, *supra* note 4, at 318 ("Monitoring is key to some safety initiatives and better safety means lower insurance premiums and workers' compensation pay-outs."). Interestingly, despite the enhanced personal safety offered by GPS monitoring systems, even those employed in one of the most dangerous mobile professions—police officers—would rather risk being alone and injured if the alternative is invasive surveillance. *See* Geoffrey James, *Can't Hide Your Prying Eyes*, COMPUTERWORLD, Mar. 1, 2004, http://www.computerworld.com/printthis/2004/0,4814,90518,00.html (describing the Orlando Police Department's failed attempt to pilot an officer surveillance program).

working environment simply because their employees are not in the workplace, and GPS surveillance offers one way to better manage this potential liability.

Second, GPS systems can significantly improve the efficiency of an employer's fleet management practices by helping to identify unproductive employees,[63] eliminate wasteful service routes,[64] and recover stolen property—especially vehicles.[65] Services such as FleetBoss can significantly lower fuel costs by helping employers control vehicle idling and speeding, which uses fuel inefficiently.[66] More dynamic routing plans can further reduce fuel costs, in addition to providing better customer service, by allowing employers to deploy the nearest available service person with very little notice.[67] Employers are not just interested in monitoring employees for sport—GPS tracking of mobile employees offers substantial savings.

D. How GPS Monitoring Has Impacted Employees

On the other hand, the substantial benefits that GPS tracking systems offer come at a cost. Scores of news stories document how GPS monitoring has disrupted the lives of numerous employees who live in fear of being dismissed for innocuous behavior that a monitoring system might distort into something more suspicious.[68]

---

[63] Schumann, *supra* note 19, at 61 ("GPS information will disclose employee abuses, such as alcohol consumption while working, deviations from routes . . . , and general shirking, and result in greater productivity.").

[64] Christopher Sherman, *Polk Keeping an Eye on the Wheels When Workers Drive the County*, ORLANDO SENTINEL, June 24, 2004, at H1 (explaining that technology can help employers "find[] the closest vehicle to a particular address" and provide better customer service).

[65] Sue Darcy, *Employers' Use of GPS Units Stirs Employee Privacy Concerns*, 175 Lab. Rel. Rep. (BNA) 212 (Aug. 30, 2004).

[66] One customer in particular, Orkin Pest Control in Atlanta, Georgia, claimed that FleetBoss helped the business save $50,000 a month on fuel costs. FleetBoss Global Positioning Solutions, Fleet Management Testimonials: Don King, http://www.fleetboss.com/testimonials.asp?REFERENCE_ID=1; *see also* GPS Fleet Solutions, CHECKMate High Resolution System, http://www.gpsfleetsolutions.com/pdfs/overviews/CHECKmate%20Presentation.pdf (last visited Sept. 28, 2005) (noting that "[r]esearch indicate[s] that each mile per hour above 50 MPH increases fuel consumption by 1.5%").

[67] FleetBoss Global Positioning Solutions, Unleashing Your Full Business Potential, http://www.fleetboss.com/oursolutions.asp (last visited September 26, 2005).

[68] Although research for this Article uncovered a few examples of GPS-related legal authority, discussed *infra* notes 75–81, "much of the evidence regarding the breadth of GPS technology use by employers and abuse of the technology is anecdotal." *Use of GPS Technology Growing, But Privacy Concerns Are Voiced*, 176 Lab. Rel. Rep. (BNA) 15 (Analysis/News and Background Information) (2004). Only five percent of companies recently surveyed by the American Management Association

For example, snowplow operators in Massachusetts[69] rallied on the capitol steps and stormed a legislative hearing in Boston to protest a new requirement that they carry GPS enabled phones.[70] In addition to their fears that the state would use surveillance data to challenge their time sheet entries, the plowers expressed concern that the technology might misinterpret idling in a traffic jam as sleeping on the job.[71] Data collected through positioning systems tells only half of the story. It provides only the "where and when" not the "why," and as the snowplowers suggested, employers might fire workers based on an assumed, perhaps inaccurate, explanation for why an employee was at a particular place for a given amount of time.[72]

Examples of discipline based on assumptions drawn from positioning data can be found in the news and in court filings. In Dallas, the owner of a car alarm installation company fired an employee after discovering, through use of a wireless tracking device, that the employee's vehicle was in the parking lot of the Million Dollar Saloon (a strip club).[73] And in *In re Superior Products Inc.*,[74] a company fired an employee when it determined, using GPS tracking data, that his late deliveries resulted, at least in part, from his failure

---

stated that "they use GPS technology to track company cell phones." *Study Concludes Most Employers Monitor Employee Internet Usage*, 177 Lab. Rel. Rep. (BNA) 138 (Analysis/News and Background Information) (2005). Lewis Maltby, president of the National Workrights Institute, concedes that "GPS use by employers is not a huge problem today," but warns that "it has the potential to become a huge problem." *Use of GPS Technology Growing, But Privacy Concerns Are Voiced*, *supra*.

[69] Note that the plowers, as state employees, could have raised objections to surveillance practices that would not apply in the context of private employment. *See* LANE, *supra* note 8, at 11 ("If your employer is a government body, agency, or department, then generally speaking, the protections of the Constitution (and particularly the Fourth Amendment, which prohibits unreasonable search and seizure) do apply to you."). However, an employee's discomfort with GPS surveillance and her reaction to her employer's threat to use such technology is not necessarily tempered by her legal options. As the anecdotes presented in Part II.D demonstrate, public and private employees alike chafe at the thought of being tagged and tracked. For this reason, the personal stories of both public and private employees are relevant to this discussion.

[70] Charles Forelle, *On the Road Again, But Now the Boss Is Sitting Beside You*, WALL ST. J., May 14, 2004, at A1.

[71] *Id.*

[72] *See infra* note 77 (discussing Senator John Edwards' concerns about how GPS tracking data can be misinterpreted).

[73] Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. TIMES, Mar. 4, 2001, § 1, at 1. Romero does not reveal whether the employee actually patronized the gentleman's club or merely happened to leave his vehicle in the vicinity of that establishment. *Id.*

[74] 116 Lab. Arb. Rep. (BNA) 1623 (2002).

to take the most direct routes.[75] The company refused to credit the employee's explanation for the detours: his supervisor owed him $87.32 in toll reimbursements and he could not afford to front additional toll costs for his employer.[76] When employers jump to conclusions about the on- and off-duty whereabouts of their employees, workers like those in these examples face harsh repercussions for what *may be* justifiable behavior.[77]

Discipline based on monitoring strictly off-duty conduct unrelated to theft or misuse of the employer's property, the focus of this Article, provides perhaps the most troubling evidence of employers' abuse of GPS services. Such actions are not only unjustifiably intrusive, but, as the situation in *Preferred Transportation, Inc.*[78] demonstrates, can also be used to mask an employer's illegal reasons for firing an employee. In *Preferred Transportation*, an employer terminated an employee for picking up extra passengers when the dispatcher ignored his calls for approval[79] and for spending

---

[75] *Id.*

[76] *Id.* at 1625.

[77] As previously suggested, *supra* text accompanying note 73, the data gathered using GPS monitoring applications encourages employers to assume the worst about their employees. When introducing the Location Privacy Protection Act, a bill aimed at restricting how companies use GPS technology to interact with their customers, *see infra* note 194, Senator John Edwards noted that "[l]ocation information is very private, sensitive information that can be misused . . . to draw inaccurate or embarrassing inferences about [people]." 147 CONG. REC. S7497 (2001). In some instances, GPS tracking systems are a blunt tool for discerning what an employee is doing. For example, what if the auto alarm employee, *see supra* note 73 and accompanying text, chose the Million Dollar Saloon parking space because the lot at a nearby grocery store was full? This hardly justifies termination.

Furthermore, technology can malfunction and place an employee in a location she never visited. For example, one former BellSouth worker claims to have been discharged after the GPS system installed in his truck reported that the vehicle remained stationary for half a day, although written statements attested to his presence at various appointments. Adventures in Blacksburg, http://www.jazybones.com/archives/000296.php (Mar. 1, 2002, 12:16 a.m.). The same system also reported that the employee "drove to three jobs without ever starting the engine." *Id.* Admittedly, these are the claims of a disgruntled ex-employee; however, we have all experienced enough internet outages and losses of cell phone service to know that modern technology is not foolproof.

[78] No. 21-CA-33407, 2003 NLRB LEXIS 236 (May 14, 2003) (decision of the administrative law judge reproduced in full at *20).

[79] *Id.* The case involved an airport shuttle service. *Id.* While driving more than one loop around the airport without permission, as the employee had done, technically violated policy, the discharged employee and a general manager testified that a second loop was generally acceptable under certain circumstances. *Id.* Moreover, the company abolished these restrictions shortly after firing the employee. *Id.* at *31, *33. Additionally, the judge dismissed the fact that the employee made more than three stops, another policy violation, as pretext for his termination

his entire lunch *break* at Home Depot and not, as the employee reported when asked, at Boston Market *and then* Home Depot.[80] Further inquiry revealed, however, that the employee was fired for his union activities, not, as alleged, for his inaccurate account of his whereabouts *while off the company clock*.[81]

Several commentators feel that these early examples of employees wronged by GPS tracking systems are a harbinger of a new breed of wrongful employment practices. Drawing upon examples of innocent after-work activities that have cost people their jobs in the past, these authors describe how GPS tracking systems would enable employers to ascertain covertly what employees do away from the office, thus stripping them of control over the personal information they once *chose* whether or not to reveal at work. One author describes how an employee's regular stops at an AIDS clinic after work, discovered by his employer through GPS tracking technologies, might trigger dismissal.[82] Another wonders: "[W]hat if your employer decides to lay you off because you stop at McDonald's for lunch two days out of three and there's concern that the cost of providing you health insurance and medical care will be increased by your weight?"[83] Additionally, these authors predict that the situation will only get worse because "[i]ncreasingly[,] . . . the tools employers are using to gather legitimate information about how [employees are]

---

because although "three or four drivers *per week* similarly violated the policy" the company had not disciplined *anyone* for such violations in the previous year. *Id.* at *36 (emphasis added).

[80] *Id.* at *39–42.

[81] *Id.* at *2. The driver involved was not a model employee. *Id.* The court held, however, that the discrepancies between his story and the GPS data recorded were part of a scheme designed solely "as a means to entrap him" in retribution for his protected union activities. *Id.* at *9.

[82] Aaron Renenger, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549, 557 (2002). The facts of this scenario are likely based on those in *Brunner v. Al Attar*, 786 S.W.2d 784 (Tex. Ct. App. 1990). In *Brunner*, an employer fired an employee who revealed that she spent her Saturdays, Sundays, and evenings volunteering with the AIDS Foundation. He feared that her activities would "place himself, his family, and the office workers in jeopardy." *Id.* at 784–85; *see also infra* text accompanying note 97.

[83] LANE, *supra* note 8, at 200. The ACLU's study on lifestyle discrimination may have inspired Lane's example. The report notes that, driven by economics, employers have, in the past, attempted to "broaden[] the sphere of their control to include what employees do in their own homes," by "refus[ing] to hire people who drink, have high cholesterol levels, or ride motorcycles." American Civil Liberties Union, Legislative Briefing Kit: Lifestyle Discrimination (Dec. 31, 1998), http://www.aclu.org/WorkplaceRights/WorkplaceRights.cfm?ID=9080&c=34.

doing [their] job[s] are also being used to track how [they] spend [their] personal time."[84]

In response, employees have taken some steps to curb abusive GPS monitoring. Notably, UPS employees, aligned with the Teamster's Union, negotiated a clause in their collective bargaining agreement that places some limits on the company's use of information obtained via GPS receivers that are attached to trucks and scheduled to be embedded in job-related portable electronic devices.[85] Likewise, the snowplowers discussed in this section secured concessions from the state and agreed to carry GPS-enabled phones as long as they were paid based on their manually submitted time sheets.[86] But for the many non-unionized, private employees out there, these bargaining solutions are not feasible.[87] Mere promises by employers not to discipline employees based on information gathered through electronic monitoring are not always binding in the private employment at-will context,[88] and consequently these

---

[84] LANE, *supra* note 8, at 187.

[85] National Master United Parcel Service Agreement, art. 37, § 1(d) (2002), http://www.browncafe.net/public/upsnma (collective bargaining agreement between UPS and the International Brotherhood of Teamsters, effective August 1, 2002 through July 31, 2008, providing that "[n]o employee shall be disciplined for exceeding personal time based on data retrieved from the DIAD/IVIS [Delivery Information Acquisition Device] or other information technology"). The agreement also requires that "the Employer shall not in any way intimidate . . . or overly supervise any employee in the performance of his or her duties." *Id.* art. 37, § 1(a). One might assume that protection from excessive supervision would extend to off-duty conduct if it is prohibited during the workday, although the agreement does not specify this. *See also* RECORDS MGMT. ASS'N OF AUSTRALASIA, TECHNOLOGY ISSUES REPORT: OCTOBER 2004, http://www.rmaa.com.au/docs/branches/nsw/pub/TISreport/2004/TIS200410.pdf (reporting that 500 Chicago city employees worked through their unions to secure concessions "allowing workers to shut down geo-tracking features during lunch time and after hours").

[86] Forelle, *supra* note 70.

[87] James, *supra* note 62 ("Although unionized employees . . . can fight the monitoring technologies, nonunion personnel have no legal recourse in the U.S., according to James T. Bennett, a professor at George Mason University who studies workplace privacy."); *see also* Joel Cutcher-Gershenfeld & Thomas Kochan, *Taking Stock: Collective Bargaining at the Turn of the Century*, 58 INDUS. & LAB. REL. REV. 3, 3 (Oct. 2004) ("Union membership in the private sector has fallen to below 9%—essentially pre-New Deal levels."); Transport Workers Union Local 562, United We Win: A Discussion of the Crisis Facing Workers and the Labor Movement (Feb. 2003), http://www.twu562.org/unitedwewin.html (noting that only nine percent of the private workforce in the United States is unionized).

[88] *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 98, 101 (E.D. Pa. 1996) (allowing company to renege on its promise to workers to keep e-mail communications confidential and privileged, and holding that, in spite of this promise, the plaintiff's expectation of privacy was not reasonable). In the context of location monitoring, unofficial reports of broken promises not to use GPS tracking

employees have few options for recourse when their employers pry into their private lives. Part III will further explore how existing legal protections fail to set reasonable limits on private employers who use GPS monitoring technologies.

III. EXISTING OFF-DUTY EMPLOYEE PRIVACY AND ELECTRONIC MONITORING LEGAL DOCTRINES

Based on a survey of cases involving employers' investigations of employee off-duty conduct, one treatise concludes that "[g]enerally, an employer appears to have a right . . . to investigate employee off-duty conduct [when it relates to] a business interest of the employer . . . ."[89] Because the law has come to expect that employers will protect their "employees . . . and the public from wrongdoing by employees," courts have recognized a nexus between employers' business interests and employees' drug use, sexual activities, and other behavior away from the office.[90] As a result, these interests have justified "a variety of [investigative] techniques [including] surveillance, wiretapping, interviews, polygraphs, and medical examinations."[91] In addition to this right to investigate and punish business-related, after-hours conduct, very little restrains employers from discharging employees at-will for activities that the employer finds repugnant and serendipitously learns about via office banter. If these methods of investigation and the resulting consequences are currently lawful employment practices, then we have little reason to

---

devices to discipline employees already exist. ABC affiliate WJLA-TV installed GPS tracking devices "to dispatch crews quickly to breaking news, not to spy on them when they are on the road;" however, "[s]ources in the newsroom [reported that] at least two staffers [were] disciplined for using a company car for personal use or for speeding in a company car." Chris Baker, *Channel 7 Uses GPS to Dispatch its Crews*, WASH. TIMES, Jan. 23, 2003, at C11. "'We all understand we can't take the company car to go to Ocean City for the weekend. But is it OK to pick up milk or pizza on the way home? All of these things were never questioned before we got the GPS system,' one photographer said." *Id.*

[89] 1 WILLIAM E. HARTSFIELD, INVESTIGATING EMPLOYEE CONDUCT § 7:15 (2004).

[90] *Id.* (citing, among others, Smith v. Zero Defects, Inc., 980 P.2d 545, 549–50 (Idaho 1999) (recognizing an employer's interest in off-duty alcohol consumption by employees, which allegedly threatened the employer's reputation, increased absenteeism, and hurt productivity); Hougum v. Valley Mem'l Homes, 574 N.W.2d 812, 814–15, 822 (N.D. 1998) (holding that whether an ordained minister's act of masturbating in a public restroom would negatively impact his "pastoral relationship" with the residents of an assisted living facility was a question of fact preventing summary judgment); French v. United Parcel Serv., Inc., 2 F. Supp. 2d 128, 130–31 (D. Mass. 1998) (recognizing an employer's interest in an off-site, drunken, emotional outburst because this behavior called into question the soundness of a supervisory employee's judgment)).

[91] HARTSFIELD, *supra* note 89, § 7:15.

expect that plaintiffs will fare any better in cases challenging dismissals or discipline based on GPS data.

A. The Employer's Existing Dominion over Off-Duty Conduct

The law's permissive approach to employers' inquiries into employees' personal lives leaves workers with few defenses against the employer's intrusive gaze. In a world where most private employment is at-will, meaning that either the employee or the employer can terminate the relationship "at any time . . . for any reason or no reason at all,"[92] many employees mistakenly believe, perhaps because of their faith in the Constitution, that they have some right to privacy. What these innocents fail to recognize is that "every single day, tens of millions of us spend hours in offices, cubicles, kitchens, laundry rooms, and work sites where the U.S. Constitution is completely inapplicable."[93] Private employers are not bound by constitutional provisions like the Fourth Amendment's Search and Seizure Clause, which limits intrusions by government employers.[94] Admittedly, anti-discrimination laws,[95] which effectively require even private employers to adhere to the Equal Protection demands of the Fourteenth Amendment, introduce a fragment of constitutional law into the private workplace. However, most of these protections, except perhaps the protections that guard against

---

[92] Jason P. Lemons, Comment, *For Any Reason or No Reason at All: Reconciling Employment at Will with the Rights of Texas Workers After* Mission Petroleum Carriers, Inc. v. Solomon, 35 ST. MARY'S L.J. 741, 743 (citing John D. Blackburn, *Restricted Employer Discharge Rights: A Changing Concept of Employment at Will*, 17 AM. BUS. L.J. 467, 467 (1980)). The original rule, a departure from the practice in England, debuted in Horace Gay Wood's much debated piece entitled *Master and Servant* in 1877. STEVEN L. WILLBORN ET AL., EMPLOYMENT LAW CASES AND MATERIALS 79, 81 (3d ed. 2002).

[93] LANE, *supra* note 8, at 10.

[94] This Article does not address how GPS tracking might be limited in the context of public employment and often assumes that public employees would fare better than private employees under current legal conditions, given the Constitutional restraints placed on the government's ability to invade privacy. However, the Oregon Supreme Court cast doubt on this theory when it upheld the use of GPS technology to track the employer-provided vehicle of a United States Forest Service employee. State v. Meredith, 96 P.3d 342, 346 (Or. 2004) (holding that under the search and seizure clause of the state constitution "defendant did not have a protected privacy interest in keeping her location and work-related activities concealed from . . . observation by her employer [conducted using a GPS] transmitter"). The government *might* be just as free to use GPS tracking technologies as private employers. *See also infra* Part IV.A (discussing government's use of GPS technology to track criminal suspects and parolees).

[95] *See* 42 U.S.C. §§ 2000e–2000e-17 (2000) (Title VII, covering discrimination because of race, color, religion, sex, or national origin); 42 U.S.C. §§ 12101–12213 (2000) (Americans with Disabilities Act ("ADA")); 29 U.S.C. §§ 621–634 (2000) (Age Discrimination in Employment Act ("ADEA")).

religious discrimination, get at traits (race, gender, age) and not activities—unless the plaintiff can make some connection between, for example, race and a particular after-hours pursuit. Consequently, going to work each day for a private employer "is, essentially, the equivalent of traveling each day to a foreign nation"[96] where the rights we often take for granted largely do not apply.

Although restrained in narrow circumstances by tort principles and statutory exceptions that will be explored in detail in Part III.B, the employment-at-will doctrine gives private employers free reign to fire employees for a seemingly limitless number of reasons that include displeasure with how an employee spends her off-duty hours. For example, employers have fired or not hired workers for providing volunteer service at an AIDS clinic,[97] for attending law school at night,[98] and for *being* smokers.[99] Recently, an employer fired a case manager with thirteen years of commendable service "because of her membership in Women's Garden Circle, an investment group [her employer] believed to be an illegal pyramid scheme."[100] Already empowered with a right to fire employees for activities voluntarily revealed, GPS tracking services will enable employers to discover *covertly* an employee's outside interests and use these extracurriculars against him or her. While employees with a "just cause" clause in their contracts can challenge being fired for *any* reason, because employers must "demonstrate that the employee's off-duty misconduct . . . has the potential to adversely affect the business,"[101] the standard at-will employee does not have this guarantee. In general, even the exceptions to the formidable at-will-employment doctrine are unlikely to provide any shelter from the boss' prying eyes. Still, an examination of these and other legal doctrines is warranted before considering what protections the law should afford.

---

[96] LANE, *supra* note 8, at 10.

[97] Brunner v. Al Attar, 786 S.W.2d 784 (Tex. Ct. App. 1990).

[98] Scroghan v. Kraftco Corp., 551 S.W.2d 811 (Ky. Ct. App. 1977).

[99] City of N. Miami v. Kurtz, 653 So. 2d 1025, 1028 (Fla. 1995) (holding that refusing to hire applicants based on their smoking habit does not violate a constitutional right to privacy because "individuals must reveal whether they smoke in almost every aspect of life in today's society" and thus cannot assert a legitimate expectation of privacy); Mark A. Rothstein, *Refusing to Employ Smokers: Good Public Health or Bad Public Policy?*, 62 NOTRE DAME L. REV. 940, 951 (1987).

[100] Grinzi v. San Diego Hospice Corp., 14 Cal. Rptr. 3d 893 (Ct. App. 2004).

[101] Daniel J. McCoy, *Recent Privacy Law Developments Affecting the Workplace*, 788 PLI/PAT. 435, 478 (2004).

B. Existing Legal Resources and Limits on their Protections

Although largely vulnerable to the whims of his employer, the at-will employee is not totally without recourse when terminated. In addition to the anti-discrimination laws previously discussed, tort law also offers some remedies for more egregious abuses of the employer's power to fire.[102] These additional limits on the employment-at-will doctrine, however, do not clearly prevent employers from manipulating the after-hours pursuits of their employees. Recognizing this shortcoming, several states have provided statutory protection for certain off-duty activities. However, these statutes, along with the one federal law that could arguably provide employees with a scintilla of privacy, would, like their common law counterparts, fall short of protecting employees from a gratuitous program of after-hours, location-based monitoring. The following discussion further demonstrates that employees tracked during after-hours activities currently lack legal protection.

1. Common Law Doctrines

Employees may "cede control over many of their waking hours as the price of being employed by another,"[103] but the common law has developed some limits on what an employer can extract from an employee in exchange for a wage. An employer cannot order its employees to take action that undermines "the interests of the general community."[104] Nor can an employer claim immunity from privacy tort claims. Still, because "we tend to look to the market to chasten abuses of employer power,"[105] courts have been very

---

[102] Although the premise behind the employment-at-will doctrine is that both employer and employee have equal opportunity to end the relationship, this overlooks that in most cases, where an employer has many employees and an employee has but one employer, the damage an employee can do to the employer's finances by quitting pales in comparison to the damage an employer can do to an employee's financial situation by firing her. Therefore, while "at will" is often seen as equally dividing power over the employer-employee relationship, this view is somewhat blind to the reality of the dynamics in this relationship. The employer retains a great deal of "power."

[103] 2 L. CAMILLE HERBERT, EMPLOYEE PRIVACY LAW § 13:3 (2004).

[104] Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 679 (1996).

[105] Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221, 256 (1996) (explaining that this situation has come about "[n]ot [because] we value privacy less, but [because] we seem to value legal non-intervention more").

conservative in their willingness to find for employees in suits alleging violations of these common law protections.[106]

a. Employment-at-Will and Tortious Wrongful Discharge

As noted, employment-at-will is the default assumption in private employment unless the parties specify otherwise. Yet certain doctrines have weakened the once absolute power of the employer to fire "for good cause, bad cause, or no cause at all."[107] States have adopted, in various combinations,[108] up to four theories of wrongful discharge in violation of public policy. These subsets of the wrongful discharge doctrine protect employees who exercise statutory rights,[109] fulfill public obligations,[110] "report the company's unlawful conduct to a supervisor or outside authorities"[111] (whistleblowers), or refuse to commit unlawful acts.[112] Generally, these intrusions into the private employer-employee relationship have been justified because of the third-party harms that might result when employees fail to follow the law or to fulfill public duties as a result of pressure from employers.[113] An employer can thus, under common law, fire someone for any reason—except one that constitutes wrongful discharge in the given state.

However, the doctrine "has never been extended to terminations in retaliation for conduct outside the employment relationship."[114]

---

[106] *See, e.g.*, Burnham v. Karl & Gelb, P.C., 745 A.2d 178, 179 (Conn. 2000) (denying the wrongful discharge claim of a secretary who "filed an anonymous complaint with the Connecticut State Dental Association . . . alleging that the defendants engaged in unsanitary and unhealthy practices in violation of the federal Occupational Safety and Health Act"). To justify this decision, the court stated: "[W]e note our adherence to the principle that the public policy exception to the general rule allowing unfettered termination of an at-will employment relationship is a narrow one. We are mindful that courts should not lightly intervene to impair the exercise of managerial discretion or to foment unwarranted litigation." *Id.* at 182 (citation omitted; internal quotation marks omitted).

[107] Cynthia G. Dooley, Note, *Wrongful Discharge: The Public Policy Exception, the Public Concern Requirement, and Employees' Private Lives*, 11 REV. LITIG. 387, 388 (1991) (paraphrasing Payne v. W. Atl. R.R., 81 Tenn. 507 (1884)).

[108] *See, e.g.*, Brunner v. Al Attar, 786 S.W.2d 784, 785–86 (Tex. Ct. App. 1990) (observing that Texas only recognizes "two exceptions to the employment-at-will doctrine" and refusing to add to the list).

[109] *Id.* ("The classic example is filing a claim for benefits under the workers' compensation statute.").

[110] *Id.* ("The classic example is serving on jury duty.").

[111] *Id.*

[112] WILLBORN ET AL., *supra* note 92, at 150.

[113] *Id.*

[114] Bammert v. Don's Super Valu, Inc., 646 N.W.2d 365, 367 (Wis. 2002) (declining to recognize a cause of action under the public policy exception to the

Thus, the success of an employee's wrongful discharge claim challenging a dismissal for off-duty activities discovered through GPS tracking techniques would depend entirely on the willingness of the court to fit the employee's activities into one of the recognized exceptions.[115] Given how narrowly courts interpret these exceptions, this possibility seems unlikely.[116] Are employees exercising a "statutory right" if they go to a bar after work simply because alcohol consumption is legal? Does working on a political campaign after clocking out fulfill a public *obligation*, or does it merely constitute a good deed? In both instances, an employee would likely fail in a suit against his employer because courts generally look for a very specific statutory right related to employment[117] and, unlike jury duty, many volunteer activities that provide public benefits are not *obligations*.[118]

---

employment-at-will doctrine when an employer fired an employee whose husband had participated in the arrest of the employer's wife for driving while under the influence).

[115] Relying on the court to extend the public policy exception is particularly risky because courts have not applied a consistent methodology when evaluating such requests. *See* WILLBORN ET AL., *supra* note 92, at 151–52 (discussing how some courts define "public policy" more broadly than others and consequently recognize more instances of wrongful discharge); *see also* Henry H. Drummonds, *The Dance of Statutes and the Common Law: Employment, Alcohol, and Other Torts*, 36 WILLAMETTE L. REV. 939, 993 (2000) (accusing common law courts of making ad hoc determinations regarding the legal basis for common law discharge accountability).

[116] *See, e.g.*, Bigelow v. Bullard, 901 P.2d 630, 633–34 (Nev. 1995) (rejecting a claim of wrongful discharge in violation of public policy brought against an employer who allegedly fired the plaintiff for arguing that "[b]lacks have rights, too" because "the remark . . . was not made in opposition or objection to the company's supposed discriminatory policies"). Seemingly, even a practice that contravenes anti-discrimination laws may not satisfy courts' high standards for wrongful termination. As long as Bullard was not fired for refusing to participate in or interfering with his employer's racially discriminatory practices, his discharge did not violate public policy. *Id.*

[117] *See, e.g.*, Frankel v. Warwick Hotel, 881 F. Supp. 183, 186–87 (E.D. Pa. 1995) (holding that the state's divorce code was merely a "vague and general expression of the legislature's view concerning the importance of family unity" and was insufficient to support a wrongful discharge claim where the employer fired an employee who refused his employer's request that he divorce his wife); Johnson v. Carpenter Tech. Corp., 723 F. Supp. 180, 184–85 (D. Conn. 1989) (rejecting employee's wrongful discharge claim based on violation of a drug testing procedure statute for employers that was passed *after* the employee was fired for not taking a test); Karren v. Far W. Fed. Savings, 717 P.2d 1271, 1273–74 (Or. Ct. App. 1986) (firing an employee for getting engaged may have interfered with a "right to marry," but this right was a private right, unrelated to her role as an employee); *see also* Roberts v. Alan Ritchey, Inc., 962 F. Supp. 1028, 1031 (S.D. Ohio 1997) (expressing doubt that the presumption of innocence provided by statute in Ohio created a public policy that was violated when an employer discharged an employee for driving under the influence, a charge that was later dropped). Narrowly decided cases like the examples provided here made it necessary for states to enact statutes to prevent

b. Privacy Torts

Given the tortious wrongful discharge doctrine's limitations, employees scrutinized beyond reason might turn to simple tort claims for relief. The common law includes a tort for the invasion of privacy, which proscribes four types of activity: intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and false light.[119] Two of these branches, intrusion upon seclusion and public disclosure of private facts, are potentially relevant in a case involving after-hours, location-based monitoring. The former tort can be asserted against the employer while the latter might be brought against either the employer or the GPS service provider. The following subsections describe how each version of the invasion of privacy tort might apply in employee tracking cases.

(1) Unreasonable Intrusion on the Right of Seclusion

The prima facie elements of an intrusion upon seclusion claim include: "(1) an intentional invasion or intrusion; (2) that is highly offensive to a reasonable person; (3) occurring where there is a reasonable expectation of privacy."[120] Particularly relevant to an examination of a GPS monitoring case, the tortious invasion need not be physical, as "use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs"[121] also qualifies as an actionable invasion. Moreover, "[t]he

---

employees from being fired for legal off-duty activities. *See* discussion *infra* Part III.B.2.

[118] *See* Greenwood v. Taft, Stettinius & Hollister, 663 N.E.2d 1030, 1032–33 (Ohio Ct. App. 1995) (holding that dismissal for pro bono work advocating equal rights for homosexuals does not violate public policy).

[119] RESTATEMENT (SECOND) OF TORTS § 652A (1977). This provision summarizes the ways in which the right of privacy can be invaded:

> (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or
> (b) appropriation of the other's name or likeness, as stated in § 652C; or
> (c) unreasonable publicity given to the other's private life, as stated in § 652D; or
> (d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.

Id.

[120] Corbett, *supra* note 10, at 109–10 (paraphrasing RESTATEMENT (SECOND) OF TORTS § 652B (1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.")).

[121] RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

intrusion itself makes the defendant subject to liability, even though there is no [use] of the . . . information."[122]

The reasonable expectation of privacy requirement, however, impedes employees' abilities to bring intrusion upon seclusion cases against employers.[123] Logically, this result makes sense, for "so long as the individual is in a public place, it is unlikely that she can maintain an argument that there was a 'reasonable expectation of privacy.'"[124] Several courts have consequently denied privacy claims brought against employers who videotaped their employees engaged in off-duty activities that "could be seen . . . by anyone driving by."[125] Additionally, the intrusion upon seclusion tort claim can easily be undermined by employers who simply notify employees that devices with GPS tracking capabilities may watch them around the clock—thus eviscerating any reasonable expectation of privacy that an employee might otherwise have had.

Still, although "[t]he law has long recognized that there is no reasonable expectation of privacy in a public place . . . one does not reasonably expect that she will be stalked and followed."[126] Some authors have argued that case law supports a reasonable expectation of some privacy even in public places. The "mere observation of a person's public activities [might not be] an intrusion upon seclusion."[127] However, an "[overzealous] sensory observation of a

---

[122] *Id.*

[123] As one commentator observed, "Most invasion of privacy claims in the employment context fail because courts find either that there is no reasonable expectation of privacy or that the invasion would not be highly offensive to a reasonable person or both." Corbett, *supra* note 10, at 110.

[124] Karim, *supra* note 36, at 508–09.

[125] York v. Gen. Elec. Co., 759 N.E.2d 865, 868 (Ohio Ct. App. 2001) (holding that employee's privacy was not invaded when the employer, as part of an investigation of a workers' compensation claim, videotaped the employee "in his yard, driving on public streets, and walking in public places" because "these activities were . . . open to the public"); I.C.U. Investigations, Inc. v. Jones, 780 So. 2d 685, 689–90 (Ala. 2000) ("Because the activities Jones carried on in his front yard[, including his urinating,] could have been observed by any passerby, we conclude that any intrusion by ICU into Jones's privacy was not 'wrongful' and, therefore, was not actionable."); McLain v. Boise Cascade Corp., 533 P.2d 343, 345 (Or. 1975) (upholding a grant of nonsuit for an invasion of privacy claim because the "activities which were filmed could have been observed by . . . neighbors or passersby on the road").

[126] White, *supra* note 40, at 1.

[127] Sheri L. Caldwell et al., *2002 John Marshall National Moot Court Competition in Information Technology and Privacy Law: Brief for the Petitioner*, 21 J. MARSHALL J. COMPUTER & INFO. L. 59, 74 (2002) (citing Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. 1970)); *see also* HARTSFIELD, *supra* note 89, § 7:13 ("Mere gathering of information about an individual usually does not give rise to a claim for invasion of

person's activities in public . . . [might] be an actionable intrusion."[128] The possibility of success on an intrusion of seclusion claim for after-hours geographic tracking of employees therefore may not be completely foreclosed, but it is questionable at best. Moreover, an expectation that one cannot be stalked, like the more general reasonable expectation of privacy, may be just as susceptible to obliteration through notice from the employer.

(2) Publicity Given to a Private Life

Alternatively, in a case against an employer and/or the company that provides the tracking technology, the tort for publicity given to a private life might apply. The tort states in full that

> [o]ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is the kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[129]

But success on such a claim in an employee tracking case will be difficult, given the accepted definitions of "publicized" and "private life" used in an analysis of this tort.

The comments accompanying the definition of publicity given to a private life in the *Second Restatement of Torts* clearly state that "it is not an invasion of the right of privacy, within the rule stated in this Section, to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons."[130] Thus, a GPS service provider's act of supplying an employer with the information obtained from its tracking system would not constitute publicizing—even if the information was published on a website—as

---

privacy. . . . However, aggressive surveillance of even public acts can serve as grounds for an invasion of privacy claim." (citations omitted)).

[128] *Id.*; *see also* Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 383–84 (Mich. Ct. App. 1989) (examining an employee's invasion of privacy claim against his employer, where an investigator "posed as a process server for the purpose of looking around the plaintiff's home" and used a powerful camera lens to look through the plaintiff's windows. The court reasoned that "[i]t may not be objectionable to peer through an open window where the curtains are not drawn, but the use of a powerful lens to observe the interior of a home or of a subterfuge to enter a home could be found objectionable to a reasonable person."). *But see* Baggs v. Eagle-Pitcher Indus., Inc., 957 F.2d 268, 275 (6th Cir. 1992) (recognizing the right of "a Michigan employer [to] use intrusive and even objectionable means to obtain employment-related information about an employee" in a case involving an employee's refusal to take an employer-administered drug test after undercover police surveillance reported that sixty percent of employees used illegal drugs).

[129] RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[130] *Id.* cmt. a.

long as only a select group of supervisors has access to the site.[131] The wide dissemination of information, not its mere recording or discovery, triggers the protection against publicity.[132] This reality also cripples use of the publicity tort against an employer, for as long as the employer uses the tracking information only to discharge or to discipline an employee, and does not post the facts discovered in the break room for all to see, the publicity requirement will not be satisfied.[133]

Even if the publicity requirement were not an obstacle, employees suing service providers and employers would also struggle to show that the information revealed concerned the employee's private life. The *Restatement* asserts that "there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye."[134] Therefore, "[a]n individual . . . would most likely have no cause of action under the publicity tort, so long as the information

---

[131] Many of the GPS service providers allow their customers to access fleet and employee management data via the Internet. *See, e.g.*, Comet Tracker Technology, http://www.comettracker.com/technology.html.

[132] RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977) ("'Publicity,' as it is used in this Section, differs from 'publication' . . . . 'Publication,' in [other contexts], is a word of art, which includes any communication by the defendant to a third person. 'Publicity,' on the other hand, means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."); *see also* Renenger, *supra* note 82, at 557 ("Recovery is also not available if the fact the person desires to keep private is not widely circulated by a defendant, but only released to a select group of people. Thus, if an employer decides not to hire a job applicant because, through exploitation of cell-phone data, the employer discovers that the applicant makes weekly visits to an AIDS clinic, there would be no cause of action against the party who released the location data for publication of private information.").

[133] Even dissemination to a *limited* group of non-supervisory *co-workers* does not appear to constitute "publicity." *See* Shattuck-Owen v. Snowbird Corp., 16 P.3d 555, 559 (Utah 2000) (awarding summary judgment to the employer even though the employer allowed a group of ten employees to view footage capturing the plaintiff's sexual assault); *see also* Wells v. Thomas, 569 F. Supp. 426, 437–38 (E.D. Pa. 1983) (revealing the terms of an employee's discharge to two persons who did not have an employment related need for this information does not constitute "publicity" as defined in the *Restatement (Second) of Torts section 652D*); Eddy v. Brown, 715 P.2d 74, 77–78 (Okla. 1986) (holding that a discussion of plaintiff's medical condition among "*only a small group* of co-workers" did not constitute publicity of private affairs). *But see* Miller v. Motorola, Inc., 560 N.E.2d 900, 903 (Ill. App. Ct. 1990) (recognizing a cause of action for public disclosure of private facts when the publicity was not widespread because "where a special relationship exists between the plaintiff and the 'public' to whom the information has been disclosed, [as is the case among fellow employees,] the disclosure may be just as devastating to the person even though the disclosure was made to a limited number of people").

[134] RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

is collected in public areas."[135] The publicity tort suffers from the same limitation common to most of the invasion of privacy torts—one generally cannot have a reasonable expectation of privacy with regard to activities in public places. If an employee walks into a bar after work, in plain view of the community, she cannot bring an invasion of privacy claim against her teetotaler employer who tracks her movements and fires her for taking a drink.

More generally, both the common law claims discussed in this section, wrongful discharge and the invasion of privacy tort, are not fully equipped to address an employee's dismissal for after-hours activities discovered through off-duty electronic surveillance. The discussion here recognizes how these doctrines *might* be read to support some protection for an employee, but also reveals that the law would still need to evolve before tracked employees could truly rely on its protections. Waiting for common law evolution is not, however, an adequate solution to the problem presented by location-based employee tracking. "Such judicial activism would . . . be piecemeal by nature and would not provide uniform protection of workplace privacy rights. Employees who suffer similar intrusions will often receive differing protection of their privacy rights."[136] Such a solution would also be untenable from the employer's perspective, given that many employers operate in multiple states and some manage a workforce that crosses state lines. National employers would have difficultly developing programs that comply with the protections provided by various common law doctrines, assuming that state courts are ready and willing to extend their jurisprudence.

2. State Laws Protecting Legal Activity Outside of Work

Like the common law doctrines discussed in the last section, existing state laws also fail to provide protection for employees monitored after hours. State laws protecting after-work activities have effectively balanced employers' and employees' interests in some specific contexts, but the protected categories are narrow and/or full of exceptions. Additionally, state laws suffer from the same lack of uniformity as the common law. Therefore, this Article ultimately advocates for a federal solution to the employee tracking problem. However, an examination of these state laws provides some guidance on how employees' off-duty interests can be protected from employer scrutiny through targeted and balanced legislation.

---

[135] Karim, *supra* note 36, at 508.
[136] Wilborn, *supra* note 24, at 855.

At last count, nearly three-fifths of the states had some law restricting the ability of employers to take action against employees based on their pursuits after work.[137] "The statutes range from merely protecting the rights of smokers to protecting all off-duty conduct . . . ."[138] Many of these statutes were, however, enacted for the very limited purpose of providing employees with a right to use certain products not proscribed by law.[139] The few statutes that do protect a more general category of off-duty conduct tend to provide employers with an exception for conduct that conflicts with the employer's business interests.[140] As a result, even in states with more generous

---

[137] See Pagnattaro, *supra* note 58, at 629 n.9.

[138] *Id.* at 629.

[139] *See* TENN. CODE ANN. § 50-1-304(e)(2) (2003). Professor Pagnattaro provides a comprehensive list of the statutes prohibiting discharge for smoking and use of other products after hours:

> The following state[] statutes prohibit an employer from infringing on an employee's right to use tobacco products outside of work: ARIZ. REV. STAT. § 36-601.02(f) (2003); D.C. CODE ANN. § 7-1703.03 (2001); IND. CODE ANN. § 22-5-4-1 (West 2003); KY. REV. STAT. ANN. § 344.040(3) (Michie 1997); LA. REV. STAT. ANN. § 23:966 (West 2003); ME. REV. STAT. ANN. tit. 26, § 597 (West 2003); MISS. CODE ANN. § 71-7-33 (2003); N.H. REV. STAT. ANN. § 275:37-a (1999); N.J. STAT. ANN. § 34:6B-1 (West 2000); N.M. STAT. ANN. § 50-11-3 (Michie 2003); OKLA. STAT. tit. 40, § 500 (2003); OR. REV. STAT. § 659A.315 (2001); R.I. GEN. LAWS § 23-20.7.1-1.(a) (2003); S.C. CODE ANN. § 41-1-85 (Law Co-op. 2003); S.D. CODIFIED LAWS § 60-4-11 (Michie 2003); VA. CODE ANN. § 15.2-1504 (Michie 2003); W. VA. CODE § 21-3-19 (2003); WYO. STAT. ANN. § 27-9-105(a)(iv) (Michie 2002). The following states make it unlawful for an employer to punish an employee for using lawful products off-duty: 820 ILL. COMP. STAT. ANN. § 55/5 (West 1993); MINN. STAT. § 181.938 (2003); MONT. CODE ANN. § 39-2-313 (2003); NEV. REV. STAT. ANN. § 613.333 (Michie 2003); N.C. GEN. STAT. § 95-28.2 (2003); WIS. STAT. ANN. §§ 111.31, 111.35 (West 2003).

Pagnattaro, *supra* note 58, at 629 n.9. However, even these seemingly straightforward laws do not guarantee an unfettered right to use the products specified. For example, the South Dakota legislature qualified its right to smoke after hours with a bona fide occupational qualification exception. S.D. CODIFIED LAWS § 60-4-11(1) (Michie 2003). In *Wood v. South Dakota Cement Plant*, the state supreme court held that an assistant kiln operator, who would work in a dusty environment and in extreme temperatures, could be prohibited from smoking while off-duty, despite the statute's protections. 588 N.W.2d 227, 230–31 (S.D. 1999).

[140] *See* COLO. REV. STAT. § 24-34-402.5(1)(a) (2003) (declaring unlawful an employer's termination of an employee for the employee's participation "in any lawful activity off the premises of the employer during nonworking hours [that is unrelated] to a bona fide occupational requirement"); CONN. GEN. STAT. § 31-51q (West Supp. 2005) (protecting an employee's off-duty exercise of constitutional rights as long as the employee's activities "[do] not substantially or materially interfere with the employee's bona fide job performance or the working relationship between the employee and the employer"); N.Y. LAB. LAW §§ 201-d(2)(c), (3)(a) (McKinney 2003) (prohibiting dismissal for "an individual's legal recreational

off-duty activity protections, an employer could still take action against a frequent consumer of Big Macs[141] if the position at issue required a certain standard of physical health. Under these laws, an employer would need only to find a way to couch its objections to an employee's activities in business interest terms to justify using the information from a GPS monitoring system to fire an employee. In sum, these laws have effectively accomplished their goals by providing some off-duty privacy, but most are too specific to cover many of the activities that GPS monitoring might discover.[142] Even the state laws that offer broader protection are limited in ways that might undermine an employee's attempts to keep his personal activities separate from his qualifications as an employee.[143]

---

activities outside work hours, off of the employer's premises and without use of the employer's equipment or other property" unless it "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest"); N.D. CENT. CODE § 14-02.4-01 (1997) (protecting "participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer").

[141] *See supra* note 83 and accompanying text.

[142] *See supra* note 139 (listing the many laws protecting only one activity—smoking—that takes place away from the office).

[143] California appeared to have created a broad, absolute protection for after-work activities when it amended its labor code to allow the Labor Commissioner to pursue claims for lost wages resulting from discharge based on off-duty activities. CAL. LAB. CODE § 96(k) (West 2004) (providing the Labor Commissioner with the power to "take assignment of . . . claims for loss of wages as the result of demotion, suspension, or discharge for the lawful conduct occurring during non-working hours away from the employer's premises"). "Rather surprisingly, [section 96(k)] of the California Labor Code [did] not contain any exceptions, like those contained in similar statutes in New York, North Dakota and Colorado . . . ." Pagnattaro, *supra* note 58, at 647–48. But subsequent interpretation by the Attorney General severely limited the scope of the law and its usefulness. In response to a state senator's inquiry as to whether "peace officers could be disciplined for engaging in lawful activities during non-working hours if such activities were inconsistent with their duties as peace officers," the Attorney General responded that, if warranted, law enforcement may discipline officers for such activities. 83 Op. Cal. Att'y Gen. 226 (2000), 2000 WL 1514816 ("Courts have long recognized that, while the off-duty conduct of employees is generally of no legal consequence to their employers, the public expects peace officers to be 'above suspicion of violation of the very laws [they are] sworn . . . to enforce.'") (quoting Pasadena Police Officers Ass'n v. City of Pasadena, 797 P.2d 608, 611 (Cal. 1990)) (alterations in original). Although tailored to the unique role of peace officers, the opinion included a sweeping statement that "the 1999 amendment of section 96 did not create new substantive rights for employees. Rather, it established a procedural mechanism that allows the Commissioner to assert, on behalf of employees, their independently recognized constitutional rights" or other rights "exist[ing] elsewhere in the law." *Id.*

3. Electronic Communications Privacy Act of 1996

Existing federal laws covering various forms of electronic monitoring likewise cannot offer the tracked employee any relief. The Electronic Communications Privacy Act of 1996 ("ECPA")[144] is not applicable to a discussion of GPS tracking systems, although it is often discussed in analyses of other forms of employee surveillance technologies, including programs that monitor Internet use and employee e-mail.[145] "[U]nlike pen registers and other electronic trap and trace devices, the Privacy Act requirements of consent or authorization do not apply to electronic signals from a tracking device, because no communication is involved."[146] Although information about someone's whereabouts does arguably communicate information about that person, the statute specifically does not cover "any communication from a tracking device,"[147] which is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[148] Therefore, a detailed discussion of this act is not warranted. The act has limited, if any, usefulness as a tool for protecting the privacy of employees under GPS surveillance.

As this section demonstrates, existing statutes and common laws remain too narrow to encompass the situation where an employer monitors employees after hours simply to exercise more control over the personalities it employs. Thus, the law fails, at this time, to provide any shelter from the pervasive stare of GPS satellites in the employment context. However, as the next section explains, people are not similarly exposed in other contexts. An inconsistent legal framework that shields the personal errands of law-abiding citizens from the prying gaze of almost everyone *except employers* is hard to defend.

IV. HOW GPS TECHNOLOGY IS REGULATED IN OTHER CONTEXTS

Use of GPS technology to monitor people's movements has ruffled feathers outside of the employment arena as well. The technology has been used by law enforcement to track criminal

---

[144] 18 U.S.C. §§ 2510–2521, 2701–2712 (2000).

[145] *See, e.g.*, Kesan, *supra* note 4, at 295–96 (noting that the ECPA "is normally interpreted to encompass e-mail").

[146] State v. Jackson, 46 P.3d 257, 270 (Wash. Ct. App. 2002) (dismissing claims challenging use of GPS to track a criminal suspect based on state privacy law).

[147] 18 U.S.C. § 2510(12)(c) ("'electronic communication' . . . does not include . . . any communication from a tracking device (as defined in section 3117 of this title)").

[148] *Id.* § 3117(b).

suspects and parolees. Businesses that rent equipment to customers have also used GPS devices to survey the location of their property and how it is used. The legal and political worlds' responses to these various uses of GPS technology therefore offer additional ideas for how to structure a policy governing the remote supervision of employees. Right now, the law's treatment of employees most closely resembles the paradigm for acceptable uses of GPS tracking technologies in law enforcement. This section argues that the treatment of criminal suspects is a poor model for how employees should be treated.

A. Use of GPS in Law Enforcement

Currently, the law regarding the use of GPS by police officers is in flux. Law enforcement has, for some time, used a variety of sensory-enhancing aids to apprehend criminals. Consequently, many courts, analogizing GPS to other acceptable uses of technology, have no problem with officers using these devices to enforce the law more efficiently.[149] A few courts, however, have more carefully considered how GPS devices might be more intrusive than other approved tracking technologies—to the point of warranting a different doctrine.[150] Still, in most contexts, GPS tracking technology *can* be used to apprehend suspects and monitor convicted criminals.[151]

1. Monitoring Suspects

As noted, officers in the past have used other technologies to track suspects. One precursor of GPS appears to have been "the beeper," a radio transmitter that emitted periodic signals capable of being "heard" by a radio receiver.[152] Although the beeper did not resemble a GPS tracking system in form or function, it served a similar purpose: the beeper could be used to track vehicles, their operators, and virtually any object that harbored the device. Because of its widespread use, even the Supreme Court has addressed electronic tracking as part of law enforcement surveillance.

In *United States v. Knotts*,[153] law enforcement officers planted a beeper in a can of chemicals purchased by a suspected manufacturer

---

[149] *See infra* notes 152–60, 172–77 and accompanying text.

[150] *See infra* notes 168–70 and accompanying text.

[151] Schumann, *supra* note 19, at 60 ("[T]o date there is no Fourth Amendment bar to GPS track evidence.").

[152] United States v. Knotts, 460 U.S. 276, 277 (1983).

[153] 460 U.S. 276 (1983).

of illegal drugs.[154] The officers had the suspect under visual surveillance, but when they lost sight of the suspect's vehicle, they relied on the beeper to determine the location of the chemicals.[155] In rejecting the defendant's claim that this electronic surveillance violated his Fourth Amendment rights against illegal searches and seizures,[156] the Court held that "beepers are merely a more effective means of observing what is already public."[157] As long as officers do not use electronic surveillance to go where they could not legally follow, the suspect's Fourth Amendment rights remain intact.[158]

In *United States v. Karo*,[159] another case involving a beeper implanted in a can of ingredients for drugs, the Court further refined the *Knotts* rule.[160] The Court distinguished *Karo* on its facts because in *Karo*, the defendants actually brought the bugged can of chemicals into a private residence, a place that officers could not legally observe without a search warrant. Consequently, the Court held that the information obtained from the continued monitoring of the container after it left the public view could not be used against the defendant. However, the Court reversed the appellate court's suppression of evidence obtained using a search warrant that was based on the electronic surveillance data because the warrant affidavit would have still been sufficient even if the facts gleaned from unconstitutional surveillance were excluded.[161] More relevant to the discussion at hand, though, is the general rule that *Knotts* and *Karo* stand for: the government can track people right up to their front doors without violating a legally recognized privacy interest.

Recent decisions reveal that the applicability of the *Karo*/*Knotts* reasoning in a GPS tracking case remains unclear. In *State v. Jackson*,[162] the police installed GPS tracking devices on cars impounded as part of an investigation into the disappearance and

---

[154] *Id.* at 278–79.

[155] *Id.*

[156] Although Fourth Amendment rights do not apply to private employer-employee arrangements, a discussion of criminal cases is relevant to the arguments made in this Article because, as the discussion will demonstrate, in an unregulated state, an employee harassed through after-hours surveillance has rights comparable to those of criminal suspects and parolees, rather than the significantly greater protections afforded to consumers and other law-abiding groups.

[157] *Knotts*, 460 U.S. at 284.

[158] *Id.* at 284–85 (dicta).

[159] 468 U.S. 705 (1984).

[160] *Id.* at 708.

[161] *Id.* at 721 n.7.

[162] 46 P.3d 257 (Wash. App. 2002).

suspected murder of William Jackson's nine year-old daughter.[163] The appellate court rejected Jackson's challenge to the adequacy of the procedures used to obtain a warrant for installation of the tracking devices because, under *Karo*, *Knotts*, and their progeny, "no search warrant was required under the state or federal constitution to use the GPS devices . . . ."[164] Echoing the reasoning in *Knotts*, the court declared that "[t]he Fourth Amendment . . . does not prohibit use of scientific enhancements to augment sensory faculties used to observe what is already open to the public."[165]

But the Washington Supreme Court accepted Jackson's petition for review[166] and ultimately disagreed with the appellate court's analysis.[167] The court reasoned that "the GPS device does not merely augment the officers' senses, but rather provides a technological substitute for traditional visual tracking."[168] Because a GPS device can "disclose a great deal about an individual's life" by "reveal[ing] preferences, alignments, associations, personal ails, and foibles" the court held that such tracking constitutes an invasion that, when conducted without a warrant, violates the protections of the state constitution's search and seizure clause.[169] The court still upheld Jackson's conviction and sentence, however, because the officers had obtained valid warrants before installing the tracking devices.[170]

Although presently limited to an interpretation of the Washington State Constitution, *Jackson* may become the rule of law for evaluating GPS surveillance procedures under the Federal Constitution.[171] The Washington Supreme Court suggested that GPS devices differ in relevant ways from an electronic beeper, which

---

[163] *Id.* at 260–61.

[164] *Id.* at 270–72.

[165] *Id.* at 270.

[166] State v. Jackson, 62 P.3d 889 (Wash. 2003).

[167] State v. Jackson, 76 P.3d 217 (Wash. 2003).

[168] *Id.* at 223.

[169] *Id.* at 223–24. Jackson did not base his appeal on the lower court's Fourth Amendment holding and consequently, the Washington Supreme Court did not address the constitutionality of warrantless GPS tracking under the Federal Constitution.

[170] *Id.* at 220.

[171] The Washington Privacy Clause, which states "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law," WASH. CONST. art. I, § 7, is "much more restrictive than the U.S. Constitution's Fourth Amendment," Schumann, *supra* note 19, at 9. *Cf.* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

officers must actively follow in a manner similar to chasing a vehicle through the streets. In contrast, GPS goes one step further, enabling officers to "watch" a suspect for weeks at a time. Without leaving the station or putting forth much effort, officers can obtain a detailed trail of a suspect's past and present location.[172] Still, other courts have comfortably extended the beeper doctrine to GPS devices. In *United States v. McIver*,[173] the Ninth Circuit held that a warrantless use of both GPS and beeper tracking devices was not unconstitutional because tracking a vehicle "thrust into the public eye . . . does not constitute a 'search.'"[174]

2. Monitoring Parolees

Likewise, a California appellate court in *People v. Zichwic*[175] upheld law enforcement's use of GPS devices, albeit in the context of monitoring parolees and not suspects.[176] *Zichwic* concluded that attaching a GPS tracking device to a parolee's car did not require a warrant, for even if such activity could be considered a search, Zichwic's status as a parolee, and the reduced expectation of privacy that necessarily accompanies such status, justified using the device.[177] The court also observed, in dicta, that regardless of Zichwic's status as a parolee, installing a GPS tracking device on a vehicle did not constitute a search because people cannot have an "objectively reasonable expectation of privacy in what is regularly exposed to public view."[178]

But even a parolee's reduced expectation of privacy does not necessarily allow for unrestrained use of GPS tracking technology. In *State v. Chism*,[179] the trial court modified Chism's home detention conditions to include non-stop GPS surveillance.[180] Subsequently, the appellate court invalidated this order because it went beyond the

---

[172] *Jackson*, 76 P.3d at 223.

[173] 186 F.3d 1119 (9th Cir. 1999).

[174] *Id.* at 1126 (quoting New York v. Class, 475 U.S. 106, 114 (1986)); *see also* United States v. Moran, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) (holding that a suspect "ha[s] no expectation of privacy in the whereabouts of his vehicle on a public roadway" and thus the use of a GPS device to track vehicles does not implicate the Fourth Amendment).

[175] 114 Cal. Rptr. 2d 733 (2001).

[176] *Id.* at 736.

[177] *Id.* at 740 (noting that the Supreme Court has held that a probation search can be "justified by a reasonable suspicion that the probationer was engaged in criminal activity").

[178] *Id.* at 740, 742.

[179] 813 N.E.2d 402 (Ind. Ct. App. 2004).

[180] *Id.* at 408.

court's statutorily created authority to require a record of when an offender in a home detention program was and was not actually present in his home.[181] The court added that when a home detainee qualifies as a violent offender, subjected to "constant supervision . . . using . . . surveillance equipment," GPS tracking may be permissible—but this condition did not apply to Chism, a regular (not violent) offender.[182] The case then advanced to the Indiana Supreme Court, which rejected the appellate court's decision and held instead that broadcast devices are acceptable tools for monitoring all parolees.[183] As a result, this tortured case, in its entirety, embodies the legal system's struggle to find appropriate uses for GPS technology and reasonable limits on its invasive capabilities—even when the subjects of monitoring are convicted criminals.

While by no means settled,[184] the law regarding the use of GPS devices in the criminal context offers some interesting comparisons with the law regarding use of this technology to observe employees. In all instances, the acceptable use of GPS hinges on a reasonable expectation of privacy, and both Fourth Amendment law and tort law have found such an expectation unreasonable when activity takes place in the "public eye."[185] But the *Jackson* decision suggests that this assumption should be reconsidered in light of the extremely invasive nature of GPS monitoring systems. Additionally, Indiana courts have made arguments for and against the rights of *convicted felons* to statutorily created protections against overly invasive uses of GPS tracking technology. At a minimum, law abiding employees certainly deserve the same protections as criminal suspects and convicts.[186] If

---

[181] *Id.* at 409–10.

[182] *Id.* at 410–11.

[183] Chism v. State, 824 N.E.2d 334, 335 (Ind. 2005), *vacating Chism*, 813 N.E.2d 402.

[184] *See* United States v. Berry, 300 F. Supp. 2d 366, 368 (D. Md. 2004) (pondering whether the U.S. Supreme Court will extend *Knotts* and *Karo*'s beeper analysis to GPS devices but declining to "decide whether modern GPS devices effect a search and seizure").

[185] *See supra* notes 134, 174 (addressing the "public eye" argument against tort and Fourth Amendment claims, respectively).

[186] At least in the case of parolees, one can argue that GPS tracking makes sense. These devices enable more efficient and cost-effective supervision of people who were convicted of crimes and, for the term of their punishment, forfeited some of the expectations of privacy they would have enjoyed otherwise. GPS might also more effectively deter recidivism, as data recorded with a GPS device can be "cross-tabulated . . . with crime incident data being reported by participating law enforcement agencies" and "crime-mapping software can be used to pinpoint whether monitored offenders were in the vicinity of a reported crime close to the time it was committed." Cecil E. Greek, *Tracking Probationers in Space and Time: The*

society's significant interest in deterring recidivism cannot justify boundless location-based surveillance, it seems incongruous to grant employers a monitoring power greater than that of law enforcement. The interest asserted by the employer could not possibly be more substantial.[187]

B. Use of GPS by Businesses to Monitor Consumers

At least in one area, lawmakers have quickly responded to the abusive intrusions made possible by GPS tracking devices. Rental car companies created quite a stir when customers discovered that their service providers had monitored their driving patterns for the express purpose of assessing fines for misuse. Caught off guard and unaware, customers racked up hundreds, and sometimes thousands, of dollars in penalty charges. For example:

> In one case, a family picked up a car at a Payless Car Rental in San Francisco and began a 12-day road trip through several Western States. When [they] returned the vehicle, they received a $3,405 bill for violating the rental contract which prohibited them from leaving California: $1/mile for every mile driven out-of-state.

Convergence of GIS and GPS Systems, FED. PROBATION, June 2002, at 51. The criminal justice system could better control the threat posed by convicts released early from overcrowded prisons by using GPS tracking technology to more effectively apprehend members of an at-risk, and perhaps not yet fully rehabilitated, population. Unlike employers, law enforcement officers have a substantial interest in using GPS tracking devices around the clock because public safety might be enhanced.

[187] It is true that criminal suspects and parolees *might* have Fourth Amendment protections that do not apply in the world of private employment. *See supra* notes 69, 156. The law has traditionally been suspicious of government power, as evidenced by the limits the founders placed on state sponsored invasions of personal space. *See* U.S. CONST. amend. IV. In contrast, the law has favored a market-based approach for curbing employer abuses of power. Finkin, *supra* note 105, at 10; *supra* text accompanying note 105; *see also* Burnham v. Karl & Gelb, P.C., 745 A.2d 178, 182 (Conn. 2000) (expressing discomfort with interfering in the employer-employee relationship). *Contra* Richard A. Epstein, *Standing Firm, On Forbidden Grounds*, 31 SAN DIEGO L. REV. 1, 1–2 (1994) (lamenting the departure from a market-based approach to employment regulation embodied in anti-discrimination and other employment laws). However, both the constitutional and tort doctrines protecting privacy are subject to a reasonableness requirement, and allowing private employers, who *can* be held accountable for tortious invasions, to treat employees worse than paroled convicts certainly seems unreasonable. Moreover, in the context of location based services, the threat posed by a Big Brother government, as opposed to a Big Brother employer, may have been more ominous when only the government had access to GPS. But now that the system has been opened to civilian use, employers' actions can be just as invasive as the government's. *See supra* notes 29, 30, 36, 38 and accompanying text; *see also* Lever, *supra* note 14, at 219 (discussing the end of government's selective availability program, which once allowed only limited use of the satellite system by civilian operations).

> When the family complained, arguing that they didn't know they were prohibited from driving out-of-state, the company presented them with a map showing their exact route outside of California as detailed by a tracking device in the car. In addition, the company argued that the family should have known about the [system used to track them] because their contract stated that the car "might be equipped with a tracking device." . . . [But this information was] in fine print in an addendum to the contract and was never mentioned by the rental agent to the family.[188]

Similarly, American Car Rental surprised James Turner when it withdrew $450 from his account to cover three instances of speeding recorded by a GPS tracking device.[189] One commentator noted that the company imposed these penalties "even though [Turner] had received no tickets from Connecticut state troopers, and had not been able to contest the allegations in court."[190]

Motivated by this great injustice, one state quickly enacted consumer protection legislation in response. On August 25, 2004, Governor Arnold Schwarzenegger of California signed into law an amendment to the Civil Code regulations of vehicle rental agreements. The law "prohibits a rental company that uses electronic surveillance technology in its rental vehicles from using, accessing, or obtaining information relating to the renter's use of the rental vehicle that was obtained using that technology."[191] In the California

---

[188] CAL. STATE ASSEMBLY COMM. ON THE JUDICIARY, REG. SESS., BILL ANALYSIS OF A.B. 2840 (Apr. 20, 2004) [hereinafter A.B. 2840 BILL ANALYSIS].

[189] Turner v. Am. Car Rental, No. CV010456353S, 2004 WL 1888947 (Conn. Super. Ct. July 21, 2004); *see also* A.B. 2840 BILL ANALYSIS, *supra* note 188. Like the Payless family, Mr. Turner was "warned" about this practice in the fine print of his contract. *Turner*, 2004 WL 1888947, at *2 ("The lease stated there was a global positioning system (GPS) in the vehicle, and it also stated that if the plaintiff exceeded the posted speed limit he would be charged $150.00 for each such occurrence.").

[190] White, *supra* note 40, at 5. Mr. Turner eventually prevailed, however, when a jury returned a verdict in favor of his invasion of privacy claim. *Turner*, 2004 WL 1888947, at *1. The court ordered a refund of the $450 fine as well as attorney's fees. *Id.* at *2; *see also* Am. Car Rental v. Comm'r of Consumer Prot., 869 A.2d 1198, 1201 (Conn. 2005) (holding that speeding fees unrelated to the actual damage done to the car, which depends on the duration of excessive speed and not the number of times a renter exceeded the speed limit, "constitute[s] an illegal penalty and . . . an unfair trade practice offensive to public policy").

[191] Press Release, Cal. Dep't of Consumer Affairs, New Laws for California Consumers (Dec. 31, 2004), *available at* http://www.dca.ca.gov/press_releases/2004/1231.htm; *see also* Legis. Counsel's Dig., Assem. Bill 2840 (Cal. 2004). In relevant part, the law states: "A rental company may not use, access, or obtain any information relating to the renter's use of the rental vehicle that was obtained using electronic surveillance technology, except in the following circumstances . . . ." CAL. CIV. CODE § 1936(o) (West Supp. 2005).

consumer bill, notice to the customer is not enough—the state imposed a blanket ban on *any use* of GPS devices for surveillance of rental car customers.

Like employers, rental car companies also have legitimate business reasons for monitoring renters after they leave the lot. Indeed, Payless only sought "to make sure business travelers and other customers adhere[d] to in-state travel agreements . . . ."[192] Of equal, if not more, importance to the rental agency is an ability to recover lost or stolen vehicles. Additionally, because GPS systems can also provide information about miles traveled, these devices offer a convenient way to keep track of information used to maintain the fleet. The California law, however, recognizes some of these concerns and provides important exceptions that take these interests into account. Electronic surveillance technology can be used to recover vehicles and provide timely maintenance.[193] But, "[a] rental company may not use electronic surveillance technology to track a renter in order to impose fines or surcharges relating to the renter's use of the rental vehicle."[194] As Part V will describe, similar provisions in a law protecting employees from discipline for information discovered through invasive monitoring could recognize an employer's legitimate interest in fleet and personnel management, while still providing employees with reasonable privacy protections. A "balancing of interests solution," similar to the one governing the business-customer relationship, makes more sense in the context of employment—as opposed to the "one-sided, absolute power" model

---

[192] *See, e.g.*, Darcy, *supra* note 65.

[193] CAL. CIV. CODE §§ 1936(o)(1)(A)(i)–(iii), (o)(6) (West Supp. 2005).

[194] *Id.* § 1936(p). California's response to notorious instances of customer surveillance has not yet been duplicated in the federal arena or elsewhere. In 2001, Senator John Edwards proposed the "Location Privacy Protection Act of 2001." S. 1164, 107th Cong. (2001). A piece of consumer protection legislation, the bill hoped "[t]o provide for the enhanced protection of the privacy of location information of users of location-based services and applications . . . ." *Id.* If passed, the bill would have required the FCC to promulgate rules governing location-based service providers' responsibility to provide detailed notice of their customer information collection practices. *Id.* Additionally, service providers would have needed customer authorization to collect, use, or retain customer data. *Id.* The bill did not, however, progress beyond its assignment to the Committee on Commerce, Science, and Transportation. This may have been a result of unfortunate timing—"[i]n the wake of the tragedy of September 11, the attitude toward the propriety of widespread surveillance . . . markedly changed." Mark G. Young, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1018 (2002). Recent rumblings in the state legislatures suggest that we are again ready to have a discussion about sensible limits on surveillance. *See* discussion *supra* Part III.B.2 and *infra* Part V.B.

that appears to control the law enforcement-criminal suspect relationship.

V. A PROPOSAL FOR REASONABLE PROTECTION AGAINST GPS MONITORING OF EMPLOYEES

As explained in Part II, GPS tracking devices offer businesses in a range of industries an unprecedented ability to control remote operations. But this technology also creates unparalleled opportunities to invade an employee's personal life. As use of "the type of technology used in the criminal justice system to track prisoners"[195] becomes commonplace, we will lose our ability to object to these invasions, because accepted practices will redefine our "reasonable expectations."[196] Indeed, in the employment context, we have already seen privacy erode as the law has refused to protect many employee communications and after-hours activities.[197] Although this Article does not challenge these well-established doctrines regarding off-duty privacy in general, it does call for a different rule when GPS technology is involved. As the *Jackson* opinion suggested, GPS tracking systems simply put more information than necessary in the hands of those who can use it unjustly.[198]

A. Federal Laws that have Failed

Admittedly, if past efforts are any indicator of future success, then establishing a privacy right for employees, even one limited to after-hours, off-site surveillance, will be difficult to achieve. Recent legislative proposals for federal protection have not fared well.

---

[195] Michael R. Triplett, *Employee Tracking Technology Raises Privacy Concerns and Potential Employee Backlash*, 72 U.S.L.W. 2664, May 4, 2004 (quoting Cindy-Ann L. Thomas, attorney).

[196] *See infra* note 282 and accompanying text.

[197] *See supra* notes 4–5, 92–101 and accompanying text; *see also infra* note 282.

[198] *See supra* notes 166–72 and accompanying text; *see also* State v. Jackson, 76 P.3d 217 (Wash. 2003). Relevant to this discussion, the court in *Jackson* observed that:

> [T]he intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life. For example, the device can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the "wrong" side of town, the family planning clinic, the labor rally.

Id. at 262.

However, these failures provide guidance for drafting a more successful policy.

1. Privacy for Consumers and Workers Act (PCWA)

In 1993, the Privacy for Consumers and Workers Act ("PCWA") debuted in both the Senate and the House.[199] "[D]esigned to prevent abuses of electronic monitoring in the workplace,"[200] these nearly identical bills sought to prohibit "the collection, storage, analysis, or reporting of information concerning an employee's activities by means of . . . electronic observation and supervision . . . which is conducted by any method other than direct observation by another person . . . ."[201] The means designed to accomplish this end were somewhat unique, as the bills proposed a tiered system that tied acceptable monitoring practices to the tenure of a particular employee. Recognizing the employer's interest in conducting a highly scrutinized trial period of initial employment, the bills allowed random monitoring during an employee's first sixty days.[202] Periodic surveillance of entire work groups was also permissible for limited periods of time.[203] However, an employer could not randomly monitor employees with five or more years of tenure, regardless of their position.[204] Employees could petition for legal or equitable

---

[199] S. 984, 103d Cong. (1993) (introduced by Sen. Paul Simon); H.R. 1900, 103d Cong. (1993) (introduced by Rep. Pat Williams). Both bills would have applied to "any individual, corporation, partnership, labor organization, unincorporated association, or any other legal business, the Federal Government, and any State (or political subdivision thereof)." S. 984 § 2(4)(B); H.R. 1900 § 2(3)(B).

[200] H.R. REP. NO. 103-872, at 45 (1994).

[201] S. 984 § 2(2)(A); H.R. 1900 § 2(1)(A). The PCWA also attempted to plug the holes in workplace privacy protection that resulted from the adoption of the Internet as a new workplace tool. At the time, some experts believed that the ECPA's limits on intercepting electronic communications, *see* discussion *supra* notes 144–48, would not effectively stop employers from monitoring employees' e-mails because employers could rely on the exception for messages intercepted "in the ordinary course of business." *Privacy for Consumers and Workers Act: Hearing on H.R. 1900 Before the Subcomm. on Labor-Management Relations of the H. Comm. on Educ. and Labor*, 103d Cong. (1993) (testimony of Lewis L. Maltby, American Civil Liberties Union), *available at* http://www.workrights.org/issue_electronic/em_testimony_6-30-93.html. Surprisingly though, the real impediment to extending ECPA's protections to employees' e-mail communications arose from the employers' ability to store e-mail messages. According to some courts, employers who read electronically stored messages have not "intercepted" anything under the ECPA. Nathan Watson, Note, *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?*, 54 FED. COMM. L.J. 79, 82–88 (2001). The PCWA proposed to remedy this oversight.

[202] S. 984 § 5(b)(1); H.R. 1900 § 5(b)(1).

[203] S. 984 § 5(b)(2); H.R. 1900 § 5(b)(2).

[204] S. 984 § 5(b)(3); H.R. 1900 § 5(b)(3).

relief from the employer, who also faced potential civil penalties of "not more than $10,000 for each . . . violation."[205]

The proposed act also included detailed specifications for the format of the notice employers needed to give to "each employee who [would] be electronically monitored." Employers would have been required to provide prior written notice detailing: (1) "[t]he forms of electronic monitoring to be used," (2) "[t]he personal data to be collected," (3) "[t]he hours and days per calendar week that electronic monitoring will occur," (4) "[t]he use to be made of personal data collected," and (5) how the electronic monitoring will be conducted and its results evaluated.[206] The bill waived the notice requirement if the employer had a reasonable suspicion that the employee was violating criminal or civil law or acting adversely to the employer's interests.[207]

Relevant to prohibiting surveillance of an employee's after-hours activities, the PCWA also proposed an absolute ban on the intentional collection of personal data about an employee, unrelated to the employee's work—unless the employee was a customer at the time of the surveillance.[208] Given this provision and others discussed in the preceding paragraphs, had the PCWA passed, this Article might have been unnecessary. Assuming that the definition of "the employee's work" was not intended to include the indirect effects that not sleeping enough or eating poorly after hours might have on an employee's performance, the PCWA may have protected employees from an employer's intrusive look into their personal lives.[209]

However, the PCWA was not meant to be, as "the bill died . . . a 'mysterious death' in committee."[210] Some speculate that the bill's defeat stemmed from "the lobbying power behind retail, security, and restaurant interests" who pitched "electronic surveillance as a loss-prevention measure."[211] Others suggest that the rigid notice

---

[205] H.R. 1900 § 12(a)(1), (c)(1); *see also* S. 984 § 12(a)(1), (c)(1).

[206] S. 984 § 4(b); H.R. 1900 § 4(b) .

[207] S. 984 § 5(c)(1); H.R. 1900 § 5(c)(1).

[208] S. 984 § 10(a); H.R. 1900 § 10(a).

[209] Some commentators would disagree. Professor Wilborn asserts: "Even if it had passed, however, the PCWA would not [have been] sufficient. By focusing almost exclusively on providing employees with notice of employer monitoring, the proposed PCWA fail[ed] to delineate what types of monitoring [would] be inappropriate even with adequate notice." Wilborn, *supra* note 24, at 851.

[210] Corbett, *supra* note 10, at 115.

[211] Karen A. Springer, *In God We Trust; All Others Who Enter this Store Are Subject to Surveillance*, 48 FED. COMM. L.J. 187, 192 (1995) (citing newspaper accounts of criticisms from retail and security lobbyists); *see also* Jennifer J. Laabs, *Surveillances: Tool or Trap?*, PERSONNEL J., June 1992, at 96 (describing the various objections that

requirements failed to account for different business needs for monitoring, something not shared across all industries, and that this weakness caused the bill to fail on its own merits.[212] Drafters of federal limitations on after-hours monitoring of employees should seriously consider these potential obstacles to the PCWA's passage.

2. Notice of Electronic Monitoring Act (NEMA)

The similarly ill-fated Notice of Electronic Monitoring Act ("NEMA") followed the PCWA in 2000.[213] "[M]ore . . . focused" and "less ambitious" than its predecessor,[214] NEMA proposed amendments to Title II of ECPA that would have placed a simple notice requirement on electronic monitoring of employee communication in the workplace.[215] Compliance with the act required annual dissemination of information on the form of communication or computer usage to be monitored, the means for and frequency of monitoring, and the information sought and how it would be used.[216] Although "lean and mean" compared to its "bloated forefather," the PCWA,[217] NEMA also proposed significant penalties for employers, including damages recoverable by an individual employee that ranged from $5,000 to $20,000.[218]

---

industry, labor, and the U.S. Department of Labor had to an earlier version of the Privacy for Consumers and Workers Act, H.R. 1218).

[212] Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"*, 28 J. MARSHALL L. REV. 139, 171 (1994) (providing an example of how the law failed to account for various business needs and explaining that "monitoring of all employees for more than two hours per week may be justifiable and even necessary for polling and survey research organizations and telemarketing firms").

[213] H.R. 4908, 106th Cong. (2000).

[214] Charles R. Frayer, Comment, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 BUS. LAW. 857, 869 n.86 (2002).

[215] Although the act included subtitles describing sections like "Electronic monitoring in the workplace," the act only covered an "employer who intentionally, by any electronic means, reads, listens to, or otherwise monitors any wire communication, oral communication, or electronic communication of an employee of the employer, or otherwise monitors the computer usage of an employee of the employer . . . ." H.R. 4908 § 2(a)(1)(B) (proposing new language for 18 U.S.C. § 2711). Because the radio signals used to pinpoint the location of a GPS tracking device are likely beyond the definition of "electronic communication of an employee" intended by the act, the bill did not address every instance of "[e]lectronic monitoring in the workplace." *Id.*

[216] *Id.* (proposing new language for 18 U.S.C. § 2711(b)(1)–(4)).

[217] Frayer, *supra* note 214, at 869.

[218] H.R. 4908 § 2(a)(1)(B) (proposing new language for 18 U.S.C. § 2711(d)). Congress proposed an overall damages cap of $500,000 for a given violation. *Id.*

Unlike PCWA, NEMA did not offer substantive employee rights or restrict employers' abilities to monitor.[219] These shortcomings led some to classify the statute as mere "dignity legislation"—not a privacy law.[220] Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, even accused the law of being counterproductive for employees, whose reasonable expectation of privacy would be undermined by an employer's provision of notice.[221] Others, however, hailed NEMA as "part of the answer to one of the major concerns of the American public today—the loss of privacy in the face of new technology."[222] James Dempsey of the Center for Democracy and Technology noted that changes in privacy law were long overdue[223] and predicted that the law would make significant contributions to the restoration of worker privacy.[224] But eventually, the critics carried the day. In mid-September of 2000, Congress tabled NEMA because of "concerns [expressed] 'by various business and employer coalitions'" regarding "the potential for an 'increase in employment litigation . . . .'"[225]

---

[219] Watson, *supra* note 201, at 92–93 ("NEMA's language does not prohibit monitoring, but merely requires an employer to give notice before electronic monitoring occurs.").

[220] Frayer, *supra* note 214, at 869.

[221] *Notice of Electronic Monitoring Act: Hearing on H.R. 4908 Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. (2000) (testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center), 2000 WL 1268416 (warning that "an employee's claims under state common law tort theories could be undermined because employees would be effectively on notice of the monitoring practices"). However, as previously noted, even without NEMA and without notice, most employees have trouble establishing a reasonable expectation of privacy when using an employer's property or when exposed to the public eye. *See* discussion *supra* Part III.B.1.b.

[222] *Notice of Electronic Monitoring Act: Hearing on H.R. 4908 Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. (2000) (testimony of James X. Dempsey, Center for Democracy and Technology) [hereinafter Dempsey Testimony], 2000 WL 1257244.

[223] *Id.* ("It is sufficient to note that privacy laws underwent their last major update in 1986 with the enactment of the Electronic Communications Privacy Act—well before email, cellular phones, and the World Wide Web became the fixtures of business and personal lives that they are today.").

[224] *Id.*

[225] Frayer, *supra* note 214, at 871 (citations omitted); *see also Notice of Electronic Monitoring Act: Hearing on H.R. 4908 Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. (2000) (testimony of Michael Robert Overly), 2000 WL 1268419 (complaining that NEMA's notice requirements were "unduly onerous and [would] almost certainly lead to litigation as to whether or not a notice included sufficient detail"). Overly called for some form of a verification requirement, which would demonstrate that an employee had read and understood the notice and prevent at least some of the predicted unnecessary litigation. *Id.*

Congress' failure to pass the PCWA and NEMA does not bode well for future efforts to reform worker privacy law through federal legislation. Employers opposed to new restrictions can more easily target and lobby federal lawmakers, as opposed to the various state legislatures around the country.[226] However, a federal law is a superior option to the patchwork of privacy protection that will develop if state legislatures are stuck with the task of protecting employees from intrusive location-based monitoring. Several states are already at work on such laws.[227] This situation should alarm employers, who will "run[] the risk of facing different laws in various jurisdictions and uncertainty regarding which state law may govern particular [situations]."[228]

B. Current State Proposals

Although state efforts to enact some form of workplace privacy law have not fared much better than their federal counterparts,[229] this has not discouraged state lawmakers from trying.[230] In their 2003–04 sessions, California, Massachusetts, Michigan, Pennsylvania, and Virginia, among others,[231] debated some form of an employee monitoring bill. The California law would have required an employer to give notice of its intent to collect information on employee activities. GPS-enabled devices were not specifically

---

[226] *But see* Wilborn, *supra* note 24, at 862 ("Attempted legislative action on the state level has been repeatedly blocked by company threats to move their business to a state without the proposed restrictions.").

[227] *See* discussion *infra* Part V.B.

[228] Wilborn, *supra* note 24, at 862.

[229] *See, e.g.*, Corbett, *supra* note 10, at 116 ("In 2001, for the third consecutive year, the California legislature passed an electronic monitoring notice bill, and for the third time in three years [then-]Democratic Governor Gray Davis vetoed the bill [because, in his opinion, it] 'place[d] unnecessary and complicating obligations on employers.'").

[230] And in some instances, succeeding. Connecticut enacted an employee electronic monitoring bill (requiring notice only) in 1998. CONN. GEN. STAT. § 31–48(d) (West 2003). The law, however, only addresses "collection of information *on an employer's premises*" and therefore does not encompass the problem of after-hours monitoring taken up in this article. *Id.* § 31-48d(3) (emphasis added).

[231] According to Lewis Maltby, president of the National Workrights Institute, New Jersey, Illinois, Minnesota, and Alaska also considered electronic monitoring notice bills during this period. Darcy, *supra* note 65. Some of these bills primarily focused on e-mail monitoring, although the Institute felt the laws might be broad enough to encompass GPS. *Id.* In addition, Maryland recently entertained a general electronic monitoring notice bill. H.B. 686, 419th Gen. Assem., Reg. Sess. (Md. 2005). However, a discussion of every bill recently debated is not necessary. The statutes selected for discussion in the text are sufficiently illustrative of the laws being proposed, at the state level, to curb GPS tracking of employees.

mentioned; however, the act broadly applied to the use of "electronic devices." The law was strictly a notice statute—employers would have simply been required to provide a warning that specified the activities, including those not related to the employer's business, that would be monitored and a description of the information sought through this process.[232] But after passing both houses, the bill was vetoed by Governor Schwarzenegger.[233]

Michigan and Pennsylvania's draft legislation, like NEMA, specifically targeted monitoring of electronic communications and contemplated requiring companies to follow detailed notice provisions before initiating a monitoring program.[234] Virginia's proposal also relied on the provision of notice.[235] Of particular interest was the Massachusetts act, which specifically addressed after-hours surveillance and mirrored many of the provisions in the defunct PCWA. The act broadly defined "electronic monitoring" to include any means of collecting information on employee activities other than direct observation.[236] Additionally, the act barred collection of information off-site or unrelated to the employee's work.[237] This bill probably asked too much of employers, because it would have prevented them from keeping tabs on their vehicles and mobile workers during business hours. Employers will not stand for this. But employers need not worry just yet—all of these ideas have yet to make it out of committee. Still, they represent tangible evidence of support for employee privacy protections that federal laws have failed to provide.

C. Proposal for a New Federal Law

The productivity, efficiency, and quality control arguments that tipped the scales in favor of employers in other challenges to

---

[232] S.B. 1841, Reg. Sess. (Cal. 2004).

[233] California Bill Tracking, S.B. 1841, Reg. Sess., STATENET, Sept. 29, 2004, http://www.lexis.com (search citation "2003 Bill Tracking CA S.B. 1841"). Note that this was the same governor who signed into law *consumer* protections against GPS tracking just one month before. *See supra* note 191 and accompanying text.

[234] S.B. 893, 187th Gen. Assem., Reg. Sess. (Pa. 2003); S.B. 675, 92d Legis., 1st Reg. Sess. (Mich. 2003).

[235] H.B. 1887, 2003 Sess. (Va. 2003).

[236] S.B. 2190, 183d Gen. Court, Reg. Sess. § 1(a) (Mass. 2003). Senator Marc Pacheco recently reintroduced a nearly identical bill. S.B. 1117, 184th Gen. Court, Reg. Sess. (Mass. 2005).

[237] S.B. 2190, 183d Gen. Court, Reg. Sess. § 2(a) (Mass. 2003) ("An employer may use electronic surveillance to collect any information so long as: (i) the information is collected at the employer's premises and (ii) the information is confined to the employee's work.").

employee surveillance practices simply do not apply when an employer seeks to use location tracking systems to unearth information about an employee's private life. This activity goes well beyond the dangers that Congress considered when weighing the merits of both the PCWA and NEMA. When an employee "sells" her services to an employer, she does not offer as part of the package an option for the employer to engage in espionage.[238] Because common law doctrines and existing laws provide inadequate safeguards in this area, a new federal law is required.[239]

A federal law will simply better serve both employers' and employees' interests, as both groups operate in an increasingly borderless environment. Because state laws "[differ] across jurisdictions in their nature and enforcement, [they] lack the uniformity of federal law. Additionally, state law is ill-suited for regulating a technology which erases state and national borders."[240] From the employer side, "a federal statute would make compliance more efficient,"[241] while from the employee side, such a law would provide a mobile workforce with a clear understanding of their rights, regardless of location. (This assumes, of course, that ardent lobbyists will successfully arrange for a drafting that preempts state innovations in this area of the law.)[242]

Specific provisions of the law that will be both effective and politically palatable are, however, more difficult to define than the law's scope. As experience has shown, even modest privacy proposals like the PCWA and NEMA made powerful enemies in both camps.[243]

---

[238] Isajiw, *supra* note 16, at 94 ("[W]hile a person subordinates herself to her employer while at work, this subordination extends only to the performance of work-related activities. The employee sells her services to the employer and nothing more."); *see also* NAT'L WORKRIGHTS INST., *supra* note 47, at 19 ("This sort of tracking seems reminiscent of someone who is in servitude, rather than someone who is being paid for his work.").

[239] *See* discussion *supra* Part III.B; *see also* Corbett, *supra* note 10, at 103 (noting that "electronic monitoring is an area where technology has outstripped the law, leaving employees largely unprotected").

[240] Kesan, *supra* note 4, at 301.

[241] Wilborn, *supra* note 24, at 879.

[242] *Compare* 17 U.S.C. § 301(a) (2000) (Copyright Act preemption provision) ("[A]ll legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 . . . are governed exclusively by this title"), *with* H.R. 1900, 103d Cong., 1st Sess. § 15 (1993) (proposed PCWA) ("This Act shall not be construed to restrict, limit, or eliminate a requirement of a State or political subdivision of a State or a collective bargaining agreement relating to electronic monitoring which is more stringent than any requirement of this Act."). *See also infra* note 260.

[243] Corbett, *supra* note 10, at 137 ("The PCWA and NEMA would have imposed modest regulations on electronic monitoring of employees, but they were bottled up

But, if used to prohibit GPS surveillance under limited circumstances, specifically when the employee is off the clock, many of the same provisions that failed as part of the PCWA and NEMA may still find their way into the federal code. The following describes how such a law might look.

1. Notice Requirement

First and foremost, employers need to let employees know that they are under watch. In terms of content, the notice should specify what location-based tracking devices are installed, where they are installed, and what they are capable of observing. Additionally, as the PCWA experience demonstrates, the notice requirement should not include both a detailed (seven part) individual notice before *every* instance of monitoring as well as an all-inclusive general announcement that the employer plans to monitor.[244] A simple one-time provision of notice, with acknowledgment of the notice signed by the employee, should suffice. This practice will not only serve to inform the employee, but it also will provide the employer with some protection in the event that the employee tries to claim he did not know about the policy.[245] Moreover, it will take the "guesswork" out of "[h]ow often, or on what system" an employer monitors its employees.[246]

2. Technology Requirement

The employer should also either be required to provide employees with a technical and real[247] power to turn off the devices in order to cloak their off-duty activities, or at least guarantee that any off-duty observations will not be used in employment decisions.[248] Particularly when devices are not embedded in equipment of substantial value, the law should favor a system capable of being

in congressional committees by business groups."); *see also supra* notes 210–12, 220–25 and accompanying text.

[244] *See* H.R. 1900 § 4(a)–(b).

[245] As noted, the provision of notice is a double-edged sword for the employee because it deprives him of any claim to a "reasonable expectation of privacy." *See supra* note 221. However, because employees are unlikely to succeed on tort claims that involve a showing of the employee's reasonable expectation of privacy, *supra* Part III.B.1.b, this objection is moot.

[246] ORWELL, *supra* note 1, at 4.

[247] *Cf. supra* note 49.

[248] *See* discussion *infra* Parts V.C.2, V.C.3.

turned off—a feature that at least some systems currently offer.[249] This will minimize the possibility that employers will use the devices to determine an employee's extracurricular interests. Workers, like the snowplow operators in Massachusetts,[250] will likely chafe if employers use a record of when the GPS device was on and off to verify hours worked for payroll purposes. However, employee privacy protection legislation requires a critical balancing of interests as new technologies emerge that offer legitimate benefits to employers at the expense of employees' imagined right to privacy.[251] Concessions need to come from both sides to make such laws work.

3. Exceptions Limited to Legitimate Business Interest

If an employer has a legitimate and significant business interest in monitoring an *asset* in the employee's possession after hours, the new law should allow limited surveillance for the sole purpose of protecting the asset.[252] Information about an employee's legal, off-duty activity, incidentally obtained as part of this exception to a general bar on after-hours monitoring, should not be used to discipline an employee. The law should prohibit an employer from expanding the scope of permissible monitoring by fabricating some attenuated link between the activity observed and the employer's amorphous interest in "reputation" or the like.[253] Some reasonable limits must be placed on snooping. This solution merely provides non-unionized employees with a sensible protection similar to ones

---

[249] *See* Track Time with Comet Tracker, http://www.comettracker.com/time.html ("Workers log in to shifts and breaks using their phone. . . . See which workers are logged in and ready for work.").

[250] *See supra* note 70 and accompanying text.

[251] *See* Isajiw, *supra* note 16, at 96.

[252] Note that this exception would be designed to allow employers to track the after-hours whereabouts of big-ticket items such as the company car, but not cheap, easily replaceable cell phones or other low-cost equipment—items that an employee would likely agree to replace if lost in exchange for a little privacy.

[253] See *supra* note 90 and accompanying text for a discussion of the business interests that have justified employers' investigations of employees after hours. An example of suitable language for a business-relatedness provision comes from H.B. 2116, 187th Gen. Assem., Reg. Sess. (Pa. 2003): "An employer may not [use] data [collected] on an employee through electronic monitoring which is not relevant to the employee's *performance*." *Id.* (emphasis added). Drafters of new legislation could easily broaden this language to include permission to use data collected to protect company property. Alternatively, the law could borrow from the PCWA, which prohibited an employer from "tak[ing] any action against an employee on the basis of *personal* data obtained by electronic monitoring of such employee [while the employee was off-duty.]" H.R. 1900, 103d Cong. (1993) (emphasis added).

that forward-thinking unions have already secured for their members.[254]

4. Employee Access to Information

Employers should also provide interested employees with access to the information collected on their whereabouts. This provision would alleviate employee anxieties about a monitoring program and supply an inexpensive enforcement mechanism by empowering those with the greatest interest in making sure employers comply with the law with an ability to check for abuses. Providing employees with a "reasonable opportunity to review all personal data obtained by electronic monitoring of the employee,"[255] as other electronic monitoring laws have proposed, would recognize employees' legitimate fears about how and what information might be used against them without placing onerous demands on employers, many of whom are already required under various laws to provide employees with access to their personnel files.[256]

5. Enforcement Provisions

Finally, the enforcement provisions should be structured to minimize the burdens placed on employers who, in an unregulated world, could have enjoyed largely unfettered use of this technology. Like NEMA, a new law should provide both a floor for damages and a cap on the amount,[257] thus making employers more certain of the liability they risk if found in violation of the law's strictures. Similarly, "significant but not onerous,"[258] civil damages and the absence of criminal penalties would help overcome employers' fears that this law

---

[254] *See, e.g.*, *supra* note 85.

[255] H.R. 1900 § 7.

[256] *See, e.g.*, CAL. LAB. CODE § 1198.5(a) (West 2003) ("Every employee has the right to inspect the personnel records that the employer maintains relating to the employee's performance or to any grievance concerning the employee."); ME. REV. STAT. ANN. tit. 26, § 631 (2003) ("The employer shall, upon written request from an employee or former employee, provide the employee, former employee or duly authorized representative with an opportunity to review and copy the employee's personnel file."); MASS. GEN. LAWS ch. 149, § 52C (West 2004) ("Any employer receiving a written request from an employee shall provide the employee with an opportunity to review his personnel record within five business days of such request."). In total, "eighteen states make provision for employees to have access to their personnel files." Matthew W. Finkin, *Information Technology and Worker's Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 492 (2002).

[257] Recall that "damages under NEMA . . . [had] both a floor of $5,000 and a two-tier cap of $20,000 per employee and $500,000 per violation." Frayer, *supra* note 214, at 870; *see also* H.R. 4908, 106th Cong. § 2(d)(2) (2000).

[258] Dempsey Testimony, *supra* note 222.

will open them up to vast amounts of costly, needless litigation—a concern that has derailed past efforts to create employee privacy rights.[259] A narrow range of reasonable damages may also facilitate settlement and will prevent employees from dreaming up outrageous values for "privacy rights" that they might not have otherwise.[260] A conservative statute of limitations, a year or less, for example, could further limit the uncertainty regarding liability.[261]

Administration of the statute, depending on the assigned agency, could also impact how burdensome employers find new restrictions. Given the nature of the law, the Department of Labor ("DOL") and the Equal Employment Opportunity Commission ("EEOC") may be the most obvious choices for the job. However,

---

[259] *See supra* note 225. Punitive damages, even if capped as they are under Title VII and the ADA, *see* 42 U.S.C. § 1981a (2000), should not be included as this would defeat the goal to provide employers with a known set of consequences for monitoring employees after hours.

[260] Related to damages, the statute would have to address whether a court can award additional tort damages for violating a statutory duty. In the context of employment law, "the workers' compensation statute expressly excludes private tort remedies by employees against employers for workplace injury in most situations [while] statutes like Title VII, since the 1991 Civil Rights Act, expressly create tort liability." Drummonds, *supra* note 115, at 961. Professor Drummonds' article provides a cautionary tale of how courts can "create, or refuse to create, new torts out of statutory duties" when a statute remains silent on the tort remedy. *Id.* at 995.

[261] The statute of limitations for other employment laws is particularly brief. For example, under Title VII, once the alleged unlawful employment action occurs, an employee has 180 days to file a charge. 42 U.S.C. § 2000e-5(e)(1) (2000). If the aggrieved party files with a state-sponsored Fair Employment agency in lieu of the EEOC, the filing period is extended to between 240 and 300 days. *Id.*; EEOC v. Commercial Office Prods. Co., 486 U.S. 107, 112–13 (1980); Michael Selmi, *The Value of the EEOC: Reexamining the Agency's Role in Employment Discrimination Law*, 57 OHIO ST. L.J. 1, 7 & n.24 (1996) (noting that although the law states that the period for a state filing lasts 300 days, the state is assured a waivable 60-day investigation period that must conclude before the statute runs).

One remaining area of uncertainty involves attorney's fees and the costs of litigation. Because the "significant but not onerous" amount at stake might be less than the cost of representation, forcing employees to bear the costs of litigation—win or lose—might discourage them from pursuing justice. Thus, attorney's fees and costs should at least be awarded to victorious plaintiffs. However, to limit the flood of potential lawsuits to the most meritorious claims, and make the law more palatable for employers, the law might award attorney's fees to the prevailing party, as opposed to only including them in the package created for a victorious plaintiff. *Compare* 42 U.S.C. § 2000e-5(k) (2000) (allowing "the court, in its discretion, [to grant] the prevailing party, other than the [EEOC] or the United States, a reasonable attorney's fee" in a Title VII case), *with* 29 U.S.C. § 216(b) (2000) (allowing "[t]he court . . . in addition to any judgment awarded to the plaintiff or plaintiffs, [to grant] a reasonable attorney's fee to be paid by the defendant" in a Fair Labor Standards Act case), *and* 29 U.S.C. § 626 (2000) (incorporating into the ADEA, by reference, the remedies in 29 U.S.C. § 216).

because of the nature of the technology involved, the law may fit within the jurisdiction of the FCC. Each agency could have a legitimate claim to regulate in this field.

If responsibility lands with the DOL, then the agency role might be limited to rulemaking and optional investigatory activities, because, consistent with other DOL-administered statutes, plaintiffs could be allowed to file directly in court (similar to the procedures for filing the previously discussed tort actions and wrongful discharge claims[262]), without having to secure agency approval first.[263] In contrast, the EEOC, responsible for administration of the nation's anti-discrimination laws, consistently takes a more active role in lawsuits. In addition to offering employers guidance on how to comply with discrimination laws,[264] the EEOC screens cases and performs initial investigations in an attempt to assess the validity of a claim.[265] When the EEOC determines that cause exists to believe that the employer has violated the law, it attempts to reconcile the employer's and employee's interests and proceeds to trial if common ground cannot be reached.[266] If, however, the EEOC does not find cause, then the aggrieved employee receives a "right to sue" letter and has ninety days to pursue the case in federal court, without

---

[262] *See* discussion *supra* Part III.B.1.

[263] *See, e.g.*, 29 U.S.C. § 1132(1), (3) (2000) (Employee Retirement Income Security Act); 29 U.S.C. § 2617 (2000) (Family and Medical Leave Act). In several instances though, statutes administered by the DOL are enforced through complaints filed with the department rather than plaintiff-initiated lawsuits. *See, e.g.*, 38 U.S.C. § 4322 (2000) (Uniformed Services Employment and Reemployment Rights Act).

[264] Although employers in practice give credence to EEOC guidelines, perhaps because "good faith reliance on EEOC interpretations is a defense to a Title VII action," the EEOC does not have substantive rulemaking authority in all the areas it oversees. 42 U.S.C. § 2000e-12(b)(1) (2000); John S. Moot, *An Analysis of Judicial Deference to EEOC Interpretive Guidelines*, 1 ADMIN. L.J. 213, 214 n.8 (1987). While Congress endowed the EEOC with such power to aid in enforcement of the ADA, *see* 42 U.S.C. § 12116 (2000), and the ADEA, *see* 29 U.S.C. § 628 (2000), it limited the EEOC's authority under Title VII to procedural regulations, *see* Richard A. Bales, *Compulsory Employment Arbitration and the EEOC*, 27 PEPP. L. REV. 1, 4–5 & n.33 (1999) (citing 110 CONG. REC. H2575 (statement of Rep. Celler)); *see also* 42 U.S.C. § 2000e-5 (2000) (describing the EEOC's role in enforcing Title VII, which does not include authority to issue regulations); 29 C.F.R. § 1601.1–.93 (2004) (procedural regulations applicable to Title VII enforcement). Legislators would need to consider which model to follow if they assigned enforcement responsibilities for the monitoring law proposed here to the EEOC.

[265] Since 1999, the EEOC has also offered an alternative dispute resolution mediation option that "has been highly successful in resolving charges . . . ." The U.S. Equal Employment Opportunity Commission, History of the EEOC Mediation Program, http://www.eeoc.gov/mediate/history.html (Nov. 19, 2003).

[266] Selmi, *supra* note 261, at 9.

prejudice.[267] The process benefits employees who have free access to the materials collected through the EEOC's investigatory process if and when a federal suit becomes necessary. It also *might* appeal to employers, who would rather not litigate these matters if possible—although the process can be intrusive and expensive for them, as they must comply with EEOC subpoenas and site-visit requests, as well as expend additional legal fees to defend themselves, first during the administrative process, and second, in federal court lawsuits.

In creating the EEOC to manage discrimination complaints, "Congress recognized that the judicial system is not always the most efficient or best medium for resolving employment disputes,"[268] and the same principle would seem to apply to the after-hours surveillance law proposed here. Additionally, the EEOC, with its long history of separating legitimate business needs from pretexts for discrimination, might be in the best position to identify justifiable uses of monitoring technology. However, the EEOC has been characterized as a cumbersome roadblock to the timely resolution of discrimination claims.[269] Some have also argued that the EEOC administrative process is impotent, fails to keep employment disputes out of court, and only adds a wasteful layer of bureaucracy to the filing process.[270] Adding another statute to its administrative load may only further stretch its already limited resources.

Alternatively, the FCC already regulates consumer privacy in the telecommunications industry,[271] and both the Automobile Association of America and the Cellular Telecommunications and Internet

---

[267] *Id.* For a more detailed discussion of the EEOC's operating procedures, see Mary Kathryn Lynch, *The Equal Employment Opportunity Commission: Comments on the Agency and Its Role in Employment Discrimination Law*, 20 GA. J. INT'L & COMP. L. 89 (1990) and Selmi, *supra* note 261, at 1–12.

[268] Anthony P. Zana, *A Pragmatic Approach to EEOC Misconduct: Drawing a Line on Commission Bad Faith in Title VII Litigation*, 73 MISS. L.J. 289, 320 (2003).

[269] *See generally* Selmi, *supra* note 261.

[270] *See id.* at 10 ("[T]hese procedures amount to a rather strange and vacuous process—one where thousands of claims are filed at no financial cost to the plaintiff, few are truly investigated, fewer still resolved, and none of which is binding on any of the parties."). Selmi also asserts that "[the EEOC's] procedures lead to a large amount of litigation that would be unnecessary in many instances if claims were not initially processed by the agency." *Id.* at 11.

[271] *See* Wireless Communications and Public Safety Act of 1999, 42 U.S.C. § 222 (2000) (placing restrictions on telecommunications carriers' use or disclosure of customer proprietary network information ("CPNI")). *But see* U.S.W., Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (vacating FCC regulations, 47 C.F.R. § 64.2005, drafted in accordance with § 222, which required that telecommunications carriers secure affirmative customer permission to use CPNI, as opposed to requiring that customers opt out of an assumed approval to use CPNI; regulations violated First Amendment free speech protections).

Association have asked the FCC to regulate GPS tracking devices. Thus, the FCC may also assume responsibility.[272] Unlike the DOL and the EEOC, the FCC has experience with implementing laws that limit how personal information can be collected and used against people.[273] Therefore, the FCC might be in a better position to weigh the interests of both employers and employees in determining appropriate limits for the use of GPS surveillance systems in the context of employment.

As this discussion illustrates, Congress will have to debate the merits of each agency's claim to oversee administration of this law. Given the mix of technology and employment issues present in the proposed legislation, no one agency clearly trumps the others in its abilities to execute the statute's provisions. Additionally, how Congress reacts to GPS surveillance in other areas might also impact the suitability of a particular agency. For example, if the FCC administers a statute dealing with customer privacy protections, an idea proposed in the Location Privacy Protection Act of 2001,[274] then oversight in the employment context might be a natural extension of the agency's responsibilities. Then again, ultimately, this proposal deals with an employment issue, and the technology used to track employees today might not fall under the jurisdiction of the FCC of tomorrow. The appropriate solution is unclear at the time of this Article's publication.

D. Responses to Criticisms of the Proposal

Two aspects of this proposal will, admittedly, draw the ire of several commentators. First, some employment law scholars believe that, in light of an imagined end to Congressional interest in employment law, demonstrated by the lack of any new provisions since 1993, future attempts to legislate in this arena will fail. Second,

---

[272] White, *supra* note 40, at 14; Petition of the Cellular Telecommunications Industry Ass'n for a Rulemaking to Establish Fair Location Information Practices, WT No. 01-72, (FCC Nov. 22, 2000), *available at* http://svartifoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6512158796 (requesting that the FCC adopt location information privacy principles under its rulemaking authority provided by Congress in 42 U.S.C. § 222(f), (h)). Additionally, White notes that the Location Privacy Protection Act of 2001, *see supra* note 194, also proposed the FCC as the appropriate administrative agency to regulate location-based services in the consumer context. White, *supra* note 40, at 14; *see also* S. 1164, 107th Cong. § 2(6) (2001) ("It is in the public interest that the Federal Communications Commission establish comprehensive rules to protect the privacy of customers of location-based services applications . . . .").

[273] *See, e.g.*, 47 C.F.R. § 64.2005 (2005).

[274] S. 1164, 107th Cong. § 2(6) (2001).

some scholars object to the continued piecemeal development of very specific worker protections. However, neither critique should discourage the pursuit of the proposal presented here.

Although failure and backlash from industry have characterized recent attempts to legislate on employment matters,[275] the narrow scope of a statute providing after-hours protection against employee surveillance does not threaten employer interests in the same way that more general restrictions on all employee monitoring did. Employers objected to the "modest regulations" in the PCWA and NEMA because the provisions prohibited a broad range of monitoring activities that infringed on the employers' ability to run legitimate training and quality assurance programs,[276] and not because modern employers were stubbornly aligned in absolute opposition to any further regulation of the employer-employee relationship.[277] During working hours, employers have a variety of business needs that electronic monitoring devices can serve most efficiently. Indeed, even GPS devices, when used within the limits of employers' business interests, have tremendous value as tools to improve efficiency in numerous areas.[278] The after-hours protection called for in this Article simply does not tread on similar interests that employers will be willing to fight tooth and nail to defend.

Likewise, complaints that a law focused only on covert, after-hours surveillance will further fragment the already scattered body of employment law are without merit. In reality, as the discussion in the preceding paragraph illustrates, broad worker privacy protections are not politically feasible. Although, given the effort that will likely go into its passage, a comprehensive statute establishing workplace privacy rights would be ideal from the employees' perspective, if past

---

[275] Corbett, *supra* note 10, at 96 (warning that "despite the success of past employment legislation, resorting to this method of regulation too often can generate significant backlash"). Corbett argues that "[r]egardless of whether an epoch in employment law history has passed, at this point in time, individual employment rights legislation is not an appropriate response to these emerging problems." *Id.* at 95. Corbett calls instead for a "retrofit" of the common law to address a variety of workplace privacy invasions. *Id.* at 152–61.

[276] *See* Laabs, *supra* note 211; *see also* Julie A. Flannagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1278 (1994) ("[M]onitoring is an important tool to assist in proper training and to instill adherence to quality and safety guidelines.").

[277] *Contra* Corbett, *supra* note 10, at 134–35 (advising against worker privacy protections based on legislation because "employers do not like to be regulated, and they will oppose employment law, particularly legislation, which provides a concrete target when it is introduced in a legislature").

[278] See discussion *supra* Part II.C for examples of how GPS tracking systems can serve legitimate business interests.

experience is any indicator, employees may just have to settle for remedying the most egregious intrusions. Additionally, while efforts should be made to define "electronic surveillance" as broadly as possible to accommodate new technology, we cannot realistically foresee every technological development that might be used to invade an employee's after-hours solitude in the future.[279] The immediate concern is to prevent after-hours tracking of employees using GPS devices. If a more expansive definition of "electronic surveillance" will rouse employer opposition, then the proposal should stay focused on the problem at hand and remain open to amendment in the event of future technological changes.[280]

VI. CONCLUSION

GPS surveillance tools pose a new, immediate threat to the personal autonomy of employees, the likes of which we have not seen before.[281] As we explore the exciting new benefits this technology can offer, we must also embrace *some* limits on how employers use it to spy on employees. Moreover, we cannot delay this endeavor, for "individuals internalize each incremental step of encroachment, and thereby lose any sense that privacy was once possible in the encroached upon area."[282] Protection must be provided before our

---

[279] *See* Jill Yung, Comment, *Virtual Spaces Formed by Literary Works: Should Copyright or Property Rights (or Neither) Protect the Functional Integrity and Display of a Website?*, 99 NW. U. L. REV. 495, 507 n.66, 522, 536 (2004) (describing how, despite Congress' best efforts to draft a copyright law capable of addressing future technological advancements, the law has struggled to encompass issues arising in a new forum for publication: the Internet). *But see* Wilborn, *supra* note 24, at 852 (Wilborn warns that "[a]ny legislation which defines protection in terms of specific types of monitoring equipment will inevitably be rendered obsolete by newer employee-monitoring technology falling outside the scope of the legislation. Device-specific privacy protection legislation enacted by Congress in the past has had only a limited effect in protecting the privacy rights of private-sector employees.").

[280] Some might argue that new legislation should offer sweeping protections in case employee rights advocates suffer another winless decade like the one experienced from 1993 until the present. However, because recent, overly-ambitious proposals share some of the blame for their own failures, this Article proposes a fairly narrow solution to an alarming, immediate problem.

[281] *See* LANE, *supra* note 8, at x ("Employer surveillance tools no longer necessarily discriminate between work-related and personal activities, and the steady expansion of workplace surveillance is threatening the privacy of our homes.").

[282] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 844 (2002). In the context of employment, we have recently witnessed evidence of internalized encroachments. J.D. Fay, vice president of corporate affairs for @Road Inc. (a provider of fleet monitoring and other location-based services), reminds us that "'[w]hen sales groups were [first] deployed with pagers [and later, cellphones], they were out in the field thinking . . . "My boss can

notion of a personal identity, separate from our identity as an employee, fades completely.[283]

Although some might object to yet another law addressing "a particular, narrowly defined invasion,"[284] because more general protections against employee monitoring have failed to win approval, this Article advocates only for a solution to the most egregious form of employee surveillance: the after-hours location-based tracking of employees. Such protection represents a realistic attempt to establish at least some employee privacy protections. My proposal is a small step, but it is nonetheless a step in the right direction. Moreover, it would establish the line beyond which employer surveillance clearly goes too far. This would be a significant accomplishment in a field that has not seen much of a legislative response to the increasing threats to worker dignity and autonomy posed by technological advances.[285] Additionally, this proposal recognizes that employers have significant and legitimate interests that GPS tracking technologies can serve. Employees cannot realistically expect the law to completely disregard the lobbying power behind these interests, just as employers cannot expect employees to welcome Big Brother with open arms. As is often the case in the law, balancing these interests is an essential part of finding an appropriate place for GPS surveillance technology in the private workplace.

As an aside, even though the law currently poses few obstacles to the practice, employers should still carefully consider the decision to track a mobile workforce. Such activities could extend employer liability not otherwise imputable to the employer. Recall that under

---

call me at any time and he expects me to call him back!" Now we wouldn't dream of working without them' . . . ." Teicher, *supra* note 47 (alterations in original).

[283] *See* LANE, *supra* note 8, at 241 ("The challenge that we face today is not so much how to protect privacy in the workplace . . . but how to protect the personal and household privacy of people who are also workers."); *see also* 139 CONG. REC. S6123 (1993) (statement of Sen. Paul Simon in support of S. 984) ("Unless we begin now to define privacy—and in particular workplace privacy—as a value worth protecting, . . . new technologies will be upon us before we are ready for them.").

[284] Rod Dixon, *With Nowhere to Hide: Workers Are Scrambling for Privacy in the Digital Age*, 4 J. TECH. L. & POL'Y 1, ¶ 48 (Spring 1999), http://grove.ufl.edu/~techlaw/vol4/issue1/dixon.html (complaining that "[a] number of federal statutes regulate aspects of employee privacy, but each addresses only a particular, narrowly defined invasion. For example, separate federal statutes regulate the use of polygraph testing, credit reports, and medical examinations by employers. Similarly, over half of the states have statutes regulating the use of polygraphs in employment; at least fourteen limit employer drug testing plans; and nearly two dozen forbid adverse employment actions based on off-duty tobacco use. No statute, however, deals with the issue of employee privacy in a comprehensive way.").

[285] Corbett, *supra* note 10, at 93.

the doctrine of respondeat superior, an employer can incur vicarious liability for the activities of its employees, and the scope of this responsibility depends, in part, on the employer's ability to control the employee's actions.[286] "[T]he more information an employer has about its employees' activities, then the greater the scope of 'foreseeable' activity and less likely an employer will be able to argue that a particular employee was in fact [not acting within the scope of his employment]."[287] In monitoring for the purpose of reducing liability, employers who interject themselves into the off-duty personal activities of employees may inadvertently create a link to these pursuits that spawns more employer liability.[288] Furthermore, in addition to its effects on liability, employers should also consider the impact of GPS surveillance on worker morale—which studies show to be significant.[289] While the laws do not regulate GPS monitoring practices just yet, social norms and the "creepiness factor" of anything likened to Big Brother should influence employers' decisions on whether to use this technology in the meantime.

---

[286] *See supra* notes 59–62 and accompanying text.

[287] LANE, *supra* note 8, at 187.

[288] Use of GPS tracking technologies can backfire on employers in other ways as well. For example, in an unreported decision from the Commonwealth Court of Pennsylvania, three judges upheld the Unemployment Compensation Board of Review's determination that the Township of Lower Frederick owed unemployment compensation benefits to a security officer who was dismissed when his manually recorded logs did not match a GPS report on his activities. Twp. of Frederick v. Unemployment Comp. Bd. of Review, No. 739 C.D. 2004 *1–2 (Pa. Commw. Ct. Sept. 16, 2004), http://www.courts.state.pa.us/OpPosting/CWealth/unpublished/739CD04_9-16-04.pdf. The township's draconian policy required officers to log "every stop of 10 minutes or longer" and when the claimant failed to report some of his longer investigatory stops, he was terminated. *Id.* at 2. The court held that negligent reporting of on-duty activities did not constitute the "willful misconduct" sufficient to justify denial of an unemployment benefits claim. *Id.* at *7; *see also* McMaster v. Coca-Cola Bottling Co., No. C04-4642MHP, 2005 WL 289982 (N.D. Cal. Feb. 4, 2005) (requesting a refund of a $3 per day "personal use" fee assessed for use of company vans because employees carried GPS-enabled phones and were arguably on the clock); NAT'L WORKRIGHTS INST., *supra* note 47, at 9 (cautioning that after-hours monitoring may have financial implications under federal wage and hour laws because "[u]nder some circumstances, employees who are on call are considered on duty for purposes of overtime calculation").

[289] *See supra* notes 23–24 and accompanying text.