



NATIONAL WORKRIGHTS INSTITUTE

Bringing Human Rights to the Workplace

ON YOUR TRACKS: GPS TRACKING IN THE WORKPLACE

166 WALL STREET, PRINCETON N.J. 08540 • (609) 683-0313 • FAX (609) 683-1787

WWW.WORKRIGHTS.ORG

TABLE OF CONTENTS

Executive Summary	3
I. GPS Technology and Legislation	
A. The Science of GPS Technology	4
B. GPS Technology's Rising Popularity	5
C. The Status of Laws Affecting Use of GPS Technology	7
D. Ways Employers Use GPS Technology to Track Their Employees	
Cell phones	10
Vehicles	11
Badges	13
E. Turning GPS Devices Off	
Cell Phones	15
Vehicles	17
Badges	18
Self-Help	18
II. The Policy Effects of GPS Technology	19
III. The Case Law	
A. Guidelines for Approaching Workplace GPS Litigation	21
B. The Decisive Cases	23
C. The Reasonableness Evaluation	24
IV. Analogous Lines of Cases	
A. Supreme Court Cases	31
B. The California Cases	32
C. Government's Use of GPS	34
V. Secondary Sources	
1. <i>GPS Invasion of Worker Privacy</i>	37
2. <i>Privacy Rights, Public Policy, and the Employment Relationship</i>	39
3. <i>Privacy Issues in the Private-Sector Workplace</i>	40
4. <i>Invasion of Privacy: Refocusing the Tort in Private Sector Employment</i>	42
VI. Conclusion	44
Bibliography	45

EXECUTIVE SUMMARY

Ten years ago the world was adjusting to the fact that people could access information in the privacy of their own home from the World Wide Web. Today, technology has taken society to another plateau; people can be tracked wherever they go from their cell phone or car. These devices work in real time and can provide an interested party with a wealth of information about the private daily activities of every person. Just as the introduction of the Internet to the workplace created new legal and policy issues, GPS tracking in the workplace implicates a new set of privacy concerns. This report takes the reader through the current technology and law on this issue. It will first offer background information on how GPS technology works and what legislation has arisen in response to that technology. It will then evaluate the different ways GPS is being used by addressing recent media stories involving employers monitoring the physical location of their employees. Next, this report assesses ways for employees to protect their privacy, namely examining how GPS trackers can be turned off. The latter half of this report gives an overview on the current case law on this issue and identifies the balancing test that the courts have used to measure whether an employer has invaded an employee's privacy. Finally, law review articles and journals on this issue are summarized to give the reader a different perspective and an idea on the general consensus of the legal community. While the introduction of GPS technology into the workplace has yet to be addressed by the courts, there are guidelines to assessing the policy and legal implications of this type of technology and its impact on workplace privacy. The following report discusses and analyzes these issues.

I. GPS Technology and Legislation

A. The Science of GPS Technology

The Department of Defense first launched a Global Positioning Systems (GPS) satellite in 1978 and achieved a full constellation of 24 satellites in 1994, which the U.S. government has named Navstar.¹ Today, GPS is used for both civil and military purposes and is controlled by a joint civilian/military executive board of the U.S. government.² The system is maintained by the U.S. Air Force on behalf of all users.³

GPS relies on three components: a constellation of satellites (currently 27) orbiting about 20,000 km (11,500 miles) above the earth's surface which transmit ranging signals on two frequencies in the microwave part of the radio spectrum, a control segment which maintains GPS through a system of ground monitor stations and satellite upload facilities, and user receivers (civil and military).⁴ In simple terms, the GPS satellites transmit signals to the equipment on the ground. More specifically, the signals contain a pseudorandom code that identifies which satellite is transmitting the information, ephemeris data that contains information about the status of the satellite and the current date and time, and almanac data that tells the receiver where each satellite should be at any time throughout the day.⁵ The receivers use this data to determine how long it takes the signals to travel from the satellite to the receiver. The receiver then uses the speed of light (about 300,000 km per second and about the same speed at which radio waves travel) to calculate the satellites' location.⁶ By using the exact locations of four or more satellites, the receiver can determine its own latitude, longitude, and height.⁷ This process of determining

¹ See Darren Griffin, *How Does the Global Positioning System (GPS) Work?*, available at <http://www.pocketgps.co.uk/howgpsworks.php> (Sept. 5, 2002).

² See Richard B. Langley, *In Simple Terms, How Does GPS Work?*, available at <http://gge.unb.ca/Resources/HowDoesGPSWork.html> (last modified Mar. 27, 2003).

³ See *id.*

⁴ See *id.*

⁵ See Griffin, *supra* note 1.

⁶ See Langley, *supra* note 2.

⁷ See *id.*

a position from measurements of distances is known as trilateration (as opposed to triangulation, which is based on the measurement of angles).⁸

When GPS was first created, the U.S. government inserted timing errors into GPS transmissions to limit the accuracy of non-military GPS receivers to about 100 meters.⁹ This was known as Selective Availability and was eliminated in May of 2000.¹⁰ Today, the accuracy of a position determined with GPS depends on the type of receiver, but most hand-held GPS units have about a 10 to 20 meter accuracy.¹¹ If an additional receiver fixed at a nearby location is used, it is possible to obtain much higher accuracy through a method called Differential GPS (DGPS).¹² Furthermore, GPS is not affected by any weather conditions.¹³

B. GPS Technology's Rising Popularity

The increasing affordability, availability, and popularity of GPS technology nowadays cannot be overstated. With all cell phone companies now being required to offer GPS capabilities, for only a few dollars per month per user, a business can have access to an entire GPS application.¹⁴ Furthermore, it is estimated that by 2006, four out of every five new vehicles will be equipped with GPS.¹⁵ Worldwide GPS sales increased from \$3.9 billion in 2002 to \$4.7 billion in 2003, and it is projected that nonmilitary sales could be up to \$10.8 billion by 2008.¹⁶ Contributing to this growth in sales is the increase in the amount of employers who use GPS to track their employees. The tracking of employees' location information is a steadily growing practice among businesses, both big and small. "Once a pricey tool for

⁸ *See id.*

⁹ *See* Griffin, *supra* note 1.

¹⁰ *See id.*

¹¹ *See id.*

¹² *See id.*

¹³ *See* Langley, *supra* note 2.

¹⁴ *See id.*

¹⁵ *See* Stacy A. Teicher, *The Boss's Big Eye in the Sky: Companies Turn to Satellite Tracking Tech to Watch Workers*, available at http://abcnews.go.com/sections/scitech/US/GPS_spies_workers_CSM_031223.html (Dec. 23, 2003).

¹⁶ *See* Arik Hesseldahl, *War Highlights Role of GPS – Is Business Watching?*, available at http://www.mobileinfo.com/News_2003/Issue13/GPS_war.htm (last modified Apr. 16, 2003).

big-budget mobile fleets, global positioning system (GPS) technology is quickly becoming an affordable option for small businesses, such as Protec Dental Laboratories Ltd,” a company with only eight drivers.¹⁷

Affordability is not the only reason why GPS sales have gone up. Employers are finding a variety of reasons to use GPS technology in the workplace. Reasons employers give for implementing GPS tracking include lowering fuel costs for company vehicles, increasing employee efficiency by saving time through real time re-routing, and increasing productivity by increasing billable hours.¹⁸

Indeed, GPS and other location-tracking devices have popped up in every imaginable work environment. A November 2003 survey by *Lawn & Landscape* magazine found that 53.4 percent of the companies surveyed responded that they either use GPS to track all of their vehicles, use GPS to track some of their vehicles, or were considering using GPS in the future.¹⁹ 76 percent of county surveyors operated GPS equipment in 2002.²⁰ In 2003, a whopping 97 percent of local governments with populations of at least 100,000, 88 percent of those with 50,000 to 100,000 people, and 56 percent of smaller governments, jurisdictions with fewer than 50,000 people, utilized some form of geographic information system technology, including for uses such as viewing aerial photography, supporting property record management and taxation services; providing public access information; permitting services and emergency preparedness and response activities; capital planning, design, and construction; computer-aided response activities; and crime tracking and investigative activities.²¹ A different type of location tracking, nurse badges that rely on infrared light, is already installed in at least 137 health care

¹⁷ See Grant Buckler, *GPS Tracking Becomes More Affordable for Small Business*, available at <http://www.theglobeandmail.com/servlet/ArticleNews/TPPrint/LAC/20040624/TWG24/TPTechnology/?mainhub=GT> (June 24, 2004).

¹⁸ See Jane Applegate, *Are Your Employees Costing You?*, available at <http://www.entrepreneur.com/article/0,4621,289593,00.html> (May 17, 2001).

¹⁹ See Lauren Spiers, *Routing & Tracking*, available at http://www.atroad.com/corp/presscenter/downloads/lawn_landscape_1103.pdf (Nov. 2003).

²⁰ See *Point of View: What is the Status of Office of the County Surveyor Today?*, available at http://www.pobonline.com/CDA/ArticleInformation/PointOfView_Item/0,2432,87809,00.html (last modified Nov. 18, 2002).

²¹ See Dibya Sarkar, *Local Governments Use GIS*, available at <http://www.fcw.com/geb/articles/2003/1208/web-gis-12-11-03.asp> (Dec. 11, 2003).

facilities throughout the U.S.²² This is but a mere sampling of the growing prevalence of GPS technology in the workplace. Although there are many positive and legitimate uses for GPS equipment, employees must be aware of the possible invasions of privacy that come with the technology. After all, whether it be through GPS or some other form of technology, real time location-tracking of employees will continue to grow both in terms of the numbers of employees that are tracked and the types of companies that feel the need to track in the next few years.

C. The Status of Laws Affecting Use of GPS Technology

In 1996, the FCC enacted rules requiring that wireless carriers set up GPS technology to provide Automatic Location Identification (ALI). For Phase I, carriers had to be able to report the telephone number of the wireless 911 caller to a local Public Safety Answering Point (PSAP) and pinpoint the location of someone calling 911 to the nearest cell tower by April 1, 1998.²³ Cell towers can cover up to ten square miles, so this was a first step in narrowing down the possible location of a call's origin.²⁴ By October 1, 2001, carriers needed to be able to locate callers within 125 meters at least 67% of the time.²⁵ This was known as the E-911 Phase II standard and could be met through network based solutions or GPS-enabled handset solutions.²⁶ On September 15, 1999, the FCC amended its rules, requiring that wireless carriers declare a choice of network-based solutions or GPS-enabled handset solutions by October 1, 2000.²⁷ For those carriers that chose to use GPS-enabled handset solutions, accuracy had to be tightened to within 50 meters 67% of the time and 150 meters 95% of the time.²⁸ The mandate included a

²² See Cheryl Buswell-Robinson, *Tracking Devices Anger Nurses*, available at <http://www.labornotes.org/archives/1999/0599/0599b.html> (May 1999).

²³ See James C. White, *People, Not Places: A Policy Framework for Analyzing Location Privacy Issues*, available at <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf> (2003).

²⁴ See *id.*

²⁵ See Daniel R. Sovocool, *GPS Update: The FCC Sets the Table for GPS Location Technology in Wireless Phones*, available at http://www.thelenreid.com/articles/article/art_57_idx.htm (last visited July 19, 2004).

²⁶ See *id.*

²⁷ See *id.*

²⁸ See *id.*

four-year rollout schedule for Phase II, requiring that the first phones equipped with Phase II capabilities appear on October 1, 2001, and that nearly all cell phones comply by December 31, 2005.²⁹

The enabling legislation for the E911 Initiative was the Wireless Communications and Public Safety Act of 1999 (the 911 Act).³⁰ Representatives Roy Blunt and Pat Danner of Missouri pushed for the legislation in order to establish 911 as the nationwide telephone number for emergency assistance. Senator John McCain of Arizona and Senator Conrad Burns of Montana introduced the bill that would become the 911 Act on April 14, 1999. The House approved the Senate's version of the Act by a vote of 424-2, and Clinton signed it into law on October 26, 1999.³¹ The law designated 911 as the universal emergency telephone number within the United States and provided wireless providers and users of 911 emergency services with the same level of immunity previously provided to wireline providers and users. Also, in response to the fear that the new technology would be misused, the new law amended section 222 of the Communications Act of 1934 on privacy of consumer information and stated, "[W]ithout the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to call location information concerning the user of a commercial mobile service...."³²

Not completely satisfied with the language of the 911 Act, Senator John Edwards of North Carolina introduced the Location Privacy Protection Act of 2001.³³ It was referred to the Committee on Commerce, Science, and Transportation, but no action was taken on the bill in the 107th Congress.³⁴ After September 11th, the bill was not re-introduced in the 108th Congress.³⁵ The Location Privacy Act would have called for all providers of location-based services to give customers clear and conspicuous

²⁹ See Federal Communications Commission, *Enhanced 911*, at <http://www.fcc.gov/911/enhanced/> (last modified Mar. 10, 2004).

³⁰ See Implementation of 911 Act, Fourth Report and Order and Third Notice of Proposed Rulemaking, 15 F.C.C.R. 17079, para. 1, 20 Comm. Reg. (P & F) 489 (2000).

³¹ See generally H.R. 438, 106th Cong. (1999); S. 800, 106th Cong. (1999); S. Rep. No. 106-138, at 3 (1999).

³² See White, *supra* note 23.

³³ Location Privacy Protection Act of 2001, S. 1164, 107th Cong. (1999).

³⁴ See White, *supra* note 23.

³⁵ See *id.*

notice about proposed uses of their personal location data, consumers to give express authorization before their data could be used, and third parties to be restricted from disclosing location information without prior authorization.³⁶ Unfortunately, this law would have applied only to consumers and not to employees, the goal being to prevent unsolicited e-coupons from being sent to the unsuspecting yet potential customer walking by a retailer.

California State Senator Steve Peace introduced a bill, which contained a provision that could have created an invasion of privacy tort for GPS tracking and transfer of GPS information without the knowledge of the subject. Aaron Reneger of the *Hastings Law Journal* wrote that, although this provision was ultimately deleted, it had the ability to create a workable solution to the location information problem.

The deleted clause read:

“There shall be a cause of action for the unlawful disclosure of any personal information gathered by a commercial or government entity for a commercial or governmental purpose which that entity subsequently releases to a third party without express permission of the person to whom the information relates. It shall be presumed in any proceeding authorized by this section that the person to whom the information released relates has sustained damages thereby.”³⁷

As this provision would have presumed damages, it had the making to be an excellent deterrent to prevent companies who collect information from releasing that information.

Additionally, there could be financial issues under federal wage and hour laws that may be implicated by the use of GPS to monitor employees.; particularly in instances where the monitoring is occurring off-duty. Under some circumstances, employees who are on call are considered on duty for purposes of overtime calculation.

³⁶ *See id.*

³⁷ Aaron Reneger, *Satellite Tracking and The Right to Privacy*, 53 *Hastings L.J.* 549 (Jan. 2002).

D. Ways Employers Use GPS Technology to Track Their Employees

- **Cell Phones**

As mentioned earlier, a 1999 federal law required all cell phones to use Global Positioning Systems (GPS) by late 2005 to help emergency crews respond to 911 calls.³⁸ However, GPS-equipped cell phones are now being used for a variety of purposes, from worried parents tracking the whereabouts of their children to suspicious employers monitoring the location of their workers.³⁹ No federal law protects employees when their employers use this or any other type of location awareness technology.⁴⁰ This section will summarize sample incidents of employers tracking employees with GPS-equipped cell phones.

In Massachusetts, snowplow drivers demonstrated in Boston against a state order to carry \$90 GPS-enabled cell phones by sending the phones back.⁴¹ The Massachusetts highway department claimed the GPS technology would be used to determine whether the employees were driving at the optimal speed for laying down salt.⁴² In December of 2003, the drivers agreed to carry the cell phones after the Massachusetts highway department agreed not to use the equipment to squeeze hourly payments, as they are unsalaried independent contractors.⁴³

One of the earliest examples of how an employer can walk this fine line is in Chicago, where about 500 city employees now carry geo-tracking phones, mainly as a tool to increase their productivity. The phones were distributed to employees only after their unions won several concessions, including allowing workers to shut down geo-tracking features during lunch time and after hours.⁴⁴

³⁸ See John Canoni, *Employers Are Using Location Awareness Technology to Keep Track of Their Employees*, at http://www.nixonpeabody.com/publications_detail3.asp?Type=P&PAID=4&ID=486&Hot= (Jan. 8, 2004).

³⁹ See Amy Harmon, *Lost? Hiding? Your Cellphone Is Keeping Tabs*, available at <http://www.nytimes.com/2003/12/21/technology/21WATC.html> (Dec. 21, 2003).

⁴⁰ See Canoni, *supra* note 38.

⁴¹ See Teicher, *supra* note 15.

⁴² See *id.*

⁴³ See Charles Forelle, *Big Brother Is Really Watching You*, available at <http://www.ocnus.net/cgi-bin/exec/view.cgi?archive=45&num=11841> (May 14, 2004).

⁴⁴ *Id.*

Another troubling method of GPS-enabled cell phone use for tracking employees is when the employer does not inform the employees that they are being tracked. Howard Boyle, president of a fire sprinkler installation company in Woodside, New York, gave company phones to his five employees without informing them about the GPS feature.⁴⁵ Legislation introduced by Senator Schumer (the Notice of Electronic Monitoring Act) in the 106th Congress would have required employer's to give notice of electronic monitoring practices, but it has not been reintroduced. While several states have introduced bills on this issue, only the state of Connecticut requires employer's to give such notice.

Studies estimate that as many as 42 million Americans will be using some form of "location-aware" technology in 2005.⁴⁶ While there are many positive uses for GPS devices, privacy interests must also be taken into account. Daniel Sovocool, a partner at Thelen Reid & Priest LLP says, "I regularly get e-mails from employees concerned about their employers tracking their whereabouts after hours with company cars or GPS cell phones."⁴⁷ He advises workers to turn off the location tracker after hours, but in some cases, even when the devices appear to be turned off, they still emit detectable signals.⁴⁸ Indeed, the Northern California office of the ACLU recently received a complaint regarding a saleswoman who's employer was attempting to use a GPS equipped cell phone for 24 hour tracking purposes.

- **Vehicles**

An example of a public employer that utilizes vehicle-equipped GPS tracking for employees is the city of Oakland. Initiated because of gripes from residents about unsatisfactory street sweeping, the Oakland program equips every street sweeping vehicle with a GPS tracking system.⁴⁹ Road crews are also monitored so that the city knows how long it takes to fill a pothole.⁵⁰ The city argues that the people

⁴⁵ See Harmon, *supra* note 39.

⁴⁶ See *id.*

⁴⁷ Teicher, *supra* note 15.

⁴⁸ See *id.*

⁴⁹ See Judy Muller, *Worker Whereabouts: California City Monitors Employees Via Satellite Technology*, at http://www.abcnews.go.com/sections/wnt/SciTech/gps_employees_040221.html (Feb. 21, 2004).

⁵⁰ See *id.*

have a right to know where its public servants are, but the employees counter with Big Brother comparisons.⁵¹

“Oakland is just one of a number of cities across the country using GPS technology to improve worker accountability.”⁵² For example, law enforcement in Clinton Township, New Jersey, installed a GPS tracking device behind the front grilles of several patrol cars in 2001, without notifying the officers.⁵³ A sergeant was then able to catch five officers loitering over meals or hanging out in parking lots, when they had indicated in their log books that they were patrolling the streets or watching for highway speeders.⁵⁴ In King County, Washington, the municipal government is installing GPS receivers on tractors and trailers that haul solid waste between landfills and transfer stations in the name of improved efficiency.⁵⁵ In Canton Township and other parts of Wayne County, Michigan, salt truck and pothole crews are operating vehicles that are equipped with Palm Pilot-sized dashboard sensors that indicate the location of the vehicle, the speed of the vehicle, and even whether a snowplow is in the down or up position.⁵⁶ School buses in Marion County, Indiana, are now GPS-equipped.⁵⁷ In yet another street sweeper case, the city of Chula Vista, California, equipped its street sweeping vehicles with GPS.⁵⁸ The cities of Charleston, South Carolina, and Aurora, Colorado, also use GPS equipment to track garbage trucks and street sweepers and found that workers became more efficient even though the GPS was not installed specifically for employee monitoring.⁵⁹ The mere knowledge that employers could potentially be watching them was enough to cause these workers to be wary.

⁵¹ *See id.*

⁵² *Id.*

⁵³ *See* Forelle, *supra* note 43.

⁵⁴ *See id.*

⁵⁵ *See id.*

⁵⁶ *See* Kevin Brown, *Wayne Uses Satellite Maps to Fix Roads*, available at <http://www.detnews.com/2004/wayne/0402/16/c04-64235.htm> (Feb. 15, 2004).

⁵⁷ *See* Cathy Kightlinger, *Schools Looking to the Skies to Track Buses*, available at <http://www.indystar.com/articles/8/135547-9318-P.html> (Apr. 6, 2004).

⁵⁸ *See* City of Chula Vista, *Public Works – Operations*, available at http://www.chulavistaca.gov/City_Services/Community_Services/Public_Works_Operations/Admin/street_sweep.asp (last visited Aug. 2, 2004).

⁵⁹ *See* Teicher, *supra* note 15.

Privacy concerns obviously arise naturally when vehicles are being monitored, but they become even greater when employers use the technology for anything other than its stated purpose. At Washington's WJLA-TV, management installed tracking devices in station-owned vehicles ostensibly to allow editors to know where vehicles are for news-gathering purposes so that the closest crew can be dispatched, but employees claimed that the devices had been used to monitor them.⁶⁰ Employees recounted stories of managers phoning them to instruct them to drive slower or to question them about stopping at certain locations.⁶¹ To prevent this type of circumstance, the Teamsters have reached a contract with United Parcel Service allowing UPS to use GPS tracking to keep tabs on shipments but prohibiting use of data from GPS tracking for discipline purposes.⁶² The Teamsters argued that detours taken to avoid traffic jams or slick roads would otherwise be subject to supervisors' criticisms.⁶³ This is nowhere near the end for GPS use at UPS, though. In the future, UPS may also include GPS capabilities on delivery scanners, the electronic tablets that store delivery data, in order to improve customer service by being able to quickly reroute packages in transit.⁶⁴

- **Badges**

Tags and badges that carry a unique code are now being used to track nurses and their equipment.⁶⁵ The badges are slightly smaller than credit cards and are clipped onto collars, belts, or identification cards.⁶⁶ Instead of GPS technology, infrared light from the \$250 battery-powered badges is detected by sensors or receivers that are surrounded by electromagnetic fields and installed throughout the hospital or nursing home.⁶⁷ The system provides real-time information about the location of the nurse or

⁶⁰ See Frank James, *GPS Grows as Tool to Spy at Home, Work*, available at <http://www.chicagotribune.com/technology/chi-0302110306feb11,1,7768625.story> (Feb. 11, 2003).

⁶¹ See *id.*

⁶² See *id.*

⁶³ See Forelle, *supra* note 43.

⁶⁴ See *id.*

⁶⁵ See Buswell-Robinson, *supra* note 22.

⁶⁶ See Susan Trossman, *Tool or Weapon? Nurses Talk About Being 'Tracked'*, available at <http://www.nursingworld.org/tan/01marapr/tracked.htm> (Apr. 2001).

⁶⁷ See Buswell-Robinson, *supra* note 22.

equipment, and supervisors can receive printouts on the location of any of their staff at any time.⁶⁸ One company, Wescom Products, Inc., offers a technology called Intelligent Locator System that provides a history showing the last five places a person or piece of equipment was located, can group badges into as many as 32 different categories, displays the time personnel entered a location, and gives the extension for a phone in the area.⁶⁹

Nurse administrators stress the positive uses of the badges including the ability to monitor the time it takes to answer a patient call in order to increase patient satisfaction, the possibility of being able to figure out what times and locations need more staff, and the fact that the badges are equipped with a special button for nurses to press when they are threatened by patients.⁷⁰ Some nurses themselves laud the positive uses of the badges, such as the ability to quickly locate co-workers, being able to refute patients' claims that nurses are never around, and the elimination of loud overhead pages and ringing cell phones that tended to be disruptive to patients, especially at night.⁷¹ On the other hand, because the systems capture data from all over the health care facility to create a "map" of the employees' activities, these systems can also be used to bust union organizing drives and weed out whistleblowers.⁷² The systems would allow management to figure out exactly who is involved with the organizing.⁷³ Nurse researchers and theorists also contend that focusing on time efficiency is overly simplistic, or as one nurse puts it, "You can't judge nursing as if it were an assembly line."⁷⁴ Also, some nurses are concerned about any unknown health dangers that may be caused by exposure to the low-level infrared pulses emitting from the badges and the electromagnetic fields surrounding the sensors.⁷⁵ Furthermore, beyond all of this, every minute detail of the employee's life will be known by management, including the amount of time spent in such private places as the restroom or changing rooms.

⁶⁸ See *id.*

⁶⁹ See Wescom Products, Inc., *Intelligent Locator: A System Smart Enough to Find Anyone Anytime Anywhere*, available at <http://www.nursecall.com/Intelligent%20Locator%20System.htm> (last modified June 8, 2004).

⁷⁰ See *id.*

⁷¹ See Trossman, *supra* note 65.

⁷² See Buswell-Robinson, *supra* note 22.

⁷³ See *id.*

⁷⁴ See *id.*

This type of monitoring is happening across the country, from pediatric nurses at the University of California-San Francisco Medical Center to nurses at Wyckoff Hospital in Brooklyn, New York.⁷⁶ Fortunately, many nurses are fighting for their rights. Some are successful; some are not. The nurses' union at the Brooklyn hospital filed a grievance against wearing the sensors but lost that dispute in arbitration.⁷⁷ On the flip side, in order to gain all of the benefits of the tracking system without the fears of being overly monitored, the Alaska Nurses Association was able to win contract language similar to that of the Teamsters working for UPS: "The parties agree that data acquired by and preserved with the [tracking] system shall not be the sole source of information used to impose discipline or evaluate any nurse."⁷⁸ The District of Columbia Nurses Association was able to get more far-reaching contract language that stated that the system would not be used for disciplinary purposes whatsoever, that management could not track the amount of time nurses spend in rooms, and that the union has the right to see information generated by the system.⁷⁹ As the use of nurse tracking systems continues to grow, nurses need to seek similar protection.

E. Turning GPS Devices Off

This leads to the next important question: Can GPS trackers be turned off? There seems to be varying types of GPS technologies, but overall, it appears that, aside from badges, most tracking devices can be turned off.

- **Cell Phones**

On most cell phones, the GPS function can be turned off. One of the ways that GPS tracking can be turned off is by simply changing a setting or pressing a button. One Samsung model of a GPS-equipped cell phone allows the user to turn the Position Location feature on or off by changing the

⁷⁵ See Trossman, *supra* note 65.

⁷⁶ See Betsy Stark, *Every Step You Take...Companies Using Tracking Devices to Monitor Employees*, available at http://abcnews.go.com/sections/wnt/WorldNewsTonight/wnt010104_workplace_tracking_feature.html (Jan. 4, 2001).

⁷⁷ See *id.*

⁷⁸ See Trossman, *supra* note 65.

⁷⁹ See *id.*

settings.⁸⁰ Sanyo also offers this option on certain models.⁸¹ Other GPS phones are equipped with “I AM HERE” buttons, which must be pressed in order for tracking to work at all.⁸² Qualcomm offers this option on some of its phones.⁸³

However, even when the GPS option is turned off, once an emergency call is placed to 911, the GPS technology is automatically turned on.⁸⁴ Fortunately, the GPS feature is automatically turned back off when the emergency call is completed.⁸⁵ As for when the phone itself is turned off, it appears that if the battery is inserted, the phone, turned off or not, transmits its identifier signal to the wireless network every few seconds so that the network knows what cell the phone is in.⁸⁶ Thus, unless the employer in question is the wireless carrier itself, it seems unlikely that an employer would have access to this identifier signal.

It is interesting to note that GPS tracking does not always automatically start up when the phone is powered on. Another brand of GPS tracker, Xora GPS TimeTrack, when used with certain Nextel phones, does not start automatically when the phone is switched on.⁸⁷ The user must launch the application manually.⁸⁸ After the application is launched, the user then needs to enter login details through the “Preferences” screen.⁸⁹ With newer Nextel phones, however, the Xora GPS TimeTrack begins tracking the moment the user powers on the phone.⁹⁰

Fortunately, technology is being developed that would allow a cell phone user to have more options than simply turning the GPS tracker on or off. Researchers at the Bell Labs division of Lucent

⁸⁰ See *Samsung Releases GPS Phone*, at <http://slashdot.org/articles/01/10/10/2115236.shtml> (Oct. 10, 2001).

⁸¹ See *Where Am I?*, at http://www.blog.fastcompany.com/archives/2003/09/12/where_am_i.html (Sept. 12, 2003).

⁸² See Brendan I. Koerner, *Your Cellphone Is a Homing Device*, available at http://www.legalaffairs.org/issues/July-August-2003/feature_koerner_julaug03.html (Jul. 2003).

⁸³ See Brendan I. Koerner, *Dial 'P' for Paranoid*, available at <http://www.villagevoice.com/issues/0221/koerner.php> (May 28, 2002).

⁸⁴ See <http://slashdot.org/articles/01/10/10/2115236.shtml>, *supra* note 79.

⁸⁵ See *id.*

⁸⁶ See Tony Hallett, *Mobile-Tracking Start-Up Sees “Huge Rise” in Users*, available at <http://networks.silicon.com/mobile/talkback.htm?PROCESS=show&ID=20023079&AT=39120068-39024665t-40000018c> (2004).

⁸⁷ See *Frequently Asked Questions*, at <http://www.xora.com/timetrack/faq.html> (2004).

⁸⁸ See *id.*

⁸⁹ See *id.*

⁹⁰ See *id.*

Technologies are trying to find ways to allow the user to set their preferences about who can share the information on their location and when this information is shared.⁹¹ Traveling employees could then specifically allow only their bosses to locate them and only during the day but not after 5 p.m.⁹² Bell Labs hopes to make this technology available to customers by 2005.⁹³

- **Vehicles**

To track employees in vehicles, the employer must first turn on a program that can gather the GPS data and communicate it to the tracking/mapping/report program.⁹⁴ The employer's tracking equipment generally will not track when it is turned off. For example, one type of GPS technology called Trac2ME requires that the employee's car phone be turned on and the employer's Trac2ME program running in order for tracking to be used.⁹⁵ If an employee turns the phone off, the employer cannot collect any location data, also known as waypoints.⁹⁶ These waypoints are the key to GPS tracking. In order to check where a vehicle is in real time, one needs to update these waypoints every 15 minutes, and in order to be able to retrace the route of the vehicle later, one might need to update the waypoints anywhere from every 10 seconds to every one minute.⁹⁷

As for the employees driving the vehicles, it is highly unlikely that they would be able to turn off the GPS device on their end. For example, one company's vehicle tracking system called FleetAlert ties the vehicle's tracking device to the ignition.⁹⁸ Location information is automatically transmitted each

⁹¹ See Jeffrey Selingo, *Protecting the Cellphone User's Right to Hide*, available at <http://www.nytimes.com/2004/02/05/technology/circuits/05next.html?ex=1086926400&en=77b53131ef4d6527&ei=5070> (Feb. 5, 2004).

⁹² See *id.*

⁹³ See *id.*

⁹⁴ See Dave Lagergren, *Answers to Commonly Asked Questions About GPS/AVL Solutions*, at http://www.ccgroupp.us/gps_avl_faqs.htm (last modified May 27, 2004).

⁹⁵ See <http://www.futureroads.com/trac2me/>.

⁹⁶ See Lagergren, *supra* note 93.

⁹⁷ See *id.*

⁹⁸ See FleetAlert Vehicle Tracking System, available at <http://www.wirelesstelematics.com/products/fleetalert.html> (last visited July 21, 2004).

time the vehicle is turned on or off.⁹⁹ Also, when the vehicle is turned off, the FleetAlert even informs the employer the maximum speed the vehicle achieved since it was last turned on.¹⁰⁰

- **Badges**

Although badges do not rely on the transmission and gathering of GPS data, they still require a power source, and thus, they can be turned off. The badges require a battery and must be turned on in order to emit the infrared light.¹⁰¹ In addition, the sensor or receiver that is attached to the wall in a room must be functioning in order for the infrared light from the badges to be detected. One hospital that has considered employees' privacy rights, Providence St. Vincent Medical Center in Portland, Oregon, ensures its employees that no sensors or receivers will be installed in places such as staff rooms or lounges.¹⁰² Hospitals that choose to use such tracking devices should proceed similarly and only install sensors or receivers in rooms where employees generally would not expect privacy.

- **Self-Help**

Regardless, employees can still find creative ways to protect their privacy. Self-help remedies include physically damaging the telephone, removing or disabling the chip, or using a GPS jammer.¹⁰³ Jammers can feed their output directly into the phone's receiving antenna or to its immediate vicinity, thus jamming only the specific phone in question without disturbing other people's phones.¹⁰⁴ Also, some nurses who are tracked have "accidentally" dropped their badges in patients' bedpans, lost them in the toilet, or forgotten to wear them.¹⁰⁵ Undoubtedly, an employee would use such remedies at his or her own peril.

⁹⁹ See *id.*

¹⁰⁰ See *id.*

¹⁰¹ Telephone Interview with Wescom Products, Inc. (Aug. 2, 2004).

¹⁰² See Scott Mace, *Track Stars*, available at http://www.nurseweek.com/news/features/03-07/ortracker_web.asp (July 3, 2003).

¹⁰³ See *Your Cell Phone Is Probably a GPS Tracking Device*, at <http://www.interesting-people.org/archives/interesting-people/200308/msg00024.html> (Aug. 6, 2003).

¹⁰⁴ See *id.*

¹⁰⁵ See Buswell-Robinson, *supra* note 22.

II. The Policy Effects of GPS Technology

Global Positioning Systems technology in the workplace poses a serious threat to employee privacy and sense of dignity. According to Immanuel Kant, dignity is that which has intrinsic value that “admits of no equivalent.”¹⁰⁶ Many times people take for granted the inherent right to go throughout the world undetected. When an employee’s location is tracked in real time, he no longer has any real sense of privacy. His employer reviews every decision he makes, whether it is to take the dog for a walk or to go to a local town meeting. Each tracked location acts like a piece of a puzzle to the worker’s life. After tracking an employee’s location for a length of time, the employer will know that the worker leaves his home every day at 8:00am. He will know that on his way to work he stops at the local convenience store for a donut and goes to work. In addition, he will find that he takes two bathroom breaks during the day, one at 10:00 and one at 3:00. After work, it will be no secret that this employee stops to pray at his synagogue on his way home and then spends three hours at the house of his girlfriend, who happens to be an ex-employee. At the end of the day, the employer will have enough pieces of the puzzle to create a fully fleshed out picture of the off-duty life of his employee. Extremely personal and private details of an employee’s life are revealed, including their political activities, physical and mental health and relationships.

This sort of tracking seems reminiscent of someone who is in servitude, rather than someone who is being paid for his work. Soon, this worker might choose not to go to synagogue or his girlfriend’s house if he knows that his boss is watching. At this point, his boss is not only invading his privacy; he is taking away his dignity. In *Shulman v. Group W. Productions, Inc.* the court noted that in the tort of intrusion cases, “invasion of privacy is most clearly seen as an affront to individual dignity.”¹⁰⁷ When a person can no longer make her decisions based on her own thoughts and beliefs, she has lost her sense of privacy, her freedom of choice, and her dignity.

¹⁰⁶ Immanuel Kant, *General Introduction to the Metaphysics of Morals*, in GREAT BOOKS OF THE WESTERN WORLD, 275 (Robert Maynard Hutchins. Ed. And W. Hastie, trans., 1952).

¹⁰⁷ *Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 489 (Cal. 1998).

In a market economy, employers are always vigilant about ways of improving employee efficiency. The introduction of GPS monitoring in the workplace assumes it is no longer sufficient for employees to operate independently as long as they complete their work properly and timely. Such monitoring reduces employees to robots; cogs in a highly managed system designed to maximize worker productivity for every second they are at work. It removes any decision making aspect of the job; any control over the rights that free and rational beings have to act autonomously and with dignity. Employees are left to surrender the very aspects of individuality that often make them good employees. This is particularly more acute with GPS monitoring, as such monitoring by its very nature is used outside the office setting, in situations where employees have traditionally enjoyed the most autonomy and in situations that often require greater levels of independent decision making. Indeed, to date this class of employees has been relatively insulated from those employers that have instituted unreasonable time frames and impossible schedules on their more traditional employees. GPS technology not only allows employers to make genuine increases in efficiency, it allows such a class of employers to extend such oppressive tactics to a whole new class of employees as they try to squeeze an extra few minutes out of every hour by micromanaging and limiting even the most incidental of breaks. Employers who introduce GPS monitoring are likely to encourage their employees to favor quantity of work produced over the quality of work as even the most minimal discretion is removed. Even employers who do not intend on placing production increases above quality in order of importance may do so inadvertently, simply because quality is more difficult to monitor electronically. Pressure to increase productivity commonly has adverse effects on the quality of work produced. With the pressure to increase productivity leading to greater use of GPS monitoring, the very humanity of the American employee is becoming even more threatened as the workplace devolves even further into an electronic sweatshop.

GPS tracking is rarely tailored to meet individual employer demands or balanced with employee privacy concerns. Often times it is exerted as a means of control over employees and serves to diminish any sense of trust remaining between employer and employee. Frequently, employees are unaware of

their employers' tracking policies; sometimes they are unaware that they are even being monitored. Too often this type of electronic monitoring is used to intimidate and disempower workers, reducing them to mere task-fulfilling machines. Employees should have the right to choose where they go without worry of employer reprisal, especially in light of technological advances which have and continue to diminish this privacy.

III. The Case Law

A. Summary: Guidelines for Approaching Workplace GPS Litigation

While there is no case law on GPS monitoring in the workplace, there are guidelines to pursuing litigation in this area that can be derived from existing case law on workplace privacy, privacy generally and the use of technology to monitor individuals. This portion of this analysis will first outline how to approach litigation over employer use of GPS for workplace monitoring. It will then discuss the most decisive and applicable cases on this issue. These cases will lead to an evaluation of what is a "reasonable expectation of privacy" and whether GPS technology invades upon that expectation. Next, this paper depicts some cases that have already weighed privacy issues that are analogous to location-tracking technology. This section will include Supreme Court cases, the influential California electronic privacy cases, and cases that consider the government's use of GPS.

Workplace privacy cases are generally predicated on either common law or state constitutions ; nevertheless courts often borrow liberally from fourth amendment discussions regarding the definitions of privacy and expectation of privacy. Generally, courts look to balance the needs of the employer with the legitimate expectations of privacy of their employee. These two countervailing interests are evaluated in the following ways.

In determining whether workplace related monitoring violates a protected right, courts will often first evaluate whether the monitoring is job-related. (See for example *Pemberton, Cort and Johnson*)¹⁰⁸ Some courts use a nexus test to determine whether the employer's action is sufficiently related to a job function of the employee or their fitness to perform a job function. (See for example *Soroka*)¹⁰⁹ If so courts will attempt to balance the employer's need for information with the employees privacy rights. The nature of the employees job and the degree of importance of the information obtained by the employer are lengthy and fact sensitive determinations that weigh heavily towards determining whether the employer acted properly. Where the job implicates issues of safety, for example, and the nature of the information sought is directly related to ensuring that the individual is properly suited to ensure such, the employer will be in a good position to defend a claim. The employer must still show that their actions were not overbroad (*Saroka*¹¹⁰).¹¹¹

Courts have traditionally found a low expectation of privacy regarding workplace monitoring. They commonly require that the invasion of privacy is unreasonable, that it implicate highly personal information about the individual (See, for example, *Bratt*)¹¹² and in the traditional workplace setting this can be a difficult barrier to cross. Nevertheless, courts have found GPS technology to be highly invasive. (See *Jackson and Oates*).¹¹³ Under certain circumstances, even in a traditional employment setting, the use of GPS to monitor employees could meet the necessary legal standards for invasion of privacy. Monitoring that collects information regarding employee activities during breaks and their activity in sensitive areas such as rest rooms might be actionable. Outside the traditional employment setting and during hours traditionally regarded as personal, monitoring using GPS technology raises even stronger privacy concerns. Individuals have heightened expectations of privacy outside the confines of a traditional workplace. Such expectations can include public as well as private locations where technology

¹⁰⁸ Supra.

¹⁰⁹ Supra.

¹¹⁰ Supra.

¹¹¹ Supra.

¹¹² Supra.

such as GPS supplants the need for direct observation. (See *Kyllo, Shulman and Sanders*)¹¹⁴ The expectation of privacy is heavily influenced by whether the employee is given actual notice of the monitoring, the degree to which the notice is a general reservation of rights or substantive and whether the notice and monitoring are part of standing company policy. (See *French, Johnson* and section on secondary sources).¹¹⁵ The degree of intrusiveness will also be measured by the type of device that is being monitored and whether the monitoring is being conducted during a specific time period. Contrast monitoring of a garbage truck on a predetermined route during a specific time period with the monitoring of a traveling salespersons cell phone on a constant basis, for example. The degree of highly personal information that could be obtained in the latter instance is much greater. Such evaluations are often linked to the nature of the job. The ability of an employee to exercise control over the device and whether the device is made optional or mandatory by the employer may also be factors in such a determination.

In addition, please note that there could be financial issues under federal wage and hour laws. Under some circumstances, employees who are on call are considered on duty for purposes of overtime calculation.

As GPS technology proliferates in the workplace, employer practices in this area will come into greater conflict with legitimate and protected privacy rights of employees. While there is a dearth of case law specific to workplace GPS monitoring, more than sufficient case law exists to challenge such monitoring successfully under the right conditions. Such a case needs to be carefully selected with the right fact pattern. The National Workrights Institute will be happy to work with you on such challenges.

B. The Decisive Cases

¹¹³ Supra.

¹¹⁴ Supra.

¹¹⁵ Supra.

In *Pemberton v. Bethlehem Steel Corp.*,¹¹⁶ the Maryland Court of Special Appeals held that an employer could unobtrusively observe, film, or record the activities of an employee to ascertain the truthfulness of job-related worker's compensation claims. Balancing the worker's privacy rights, the court restricted an employer from intruding upon the employee's home or private places outside the workplace for reasons that were not job-related. In *Katz v. United States*¹¹⁷, the Supreme Court brought the term "reasonable expectations" into this issue. The court held that an individual could have a "reasonable" expectation of privacy of intangible things and this expectation of privacy is thus protected. Two applicable concepts come from that decision: 1) Justice Stewart's protection of public areas and 2) Justice Harlan's twofold societal requirement. Justice Stewart agreed that what a person seeks to preserve as private, even in a public place, could be constitutionally protected. However, Justice Harlan argued, in his concurrence, that constitutional protection should be provided when an individual actually expects privacy and when that expectation is one that society is prepared to recognize.

C. The Reasonableness Evaluation

The post-*Katz* case law has focused on defining the term "reasonable expectation" of privacy. From this inquiry, a test has emerged to determine the reasonableness of an employer's invasion of privacy of an employee. This test focuses on the level of the intrusiveness in comparison with the level of the employment. Therefore, this inquiry is fact sensitive and will change depending on the type of employment and the means of intrusiveness. While *Soroka* sees the test as a requirement of a reasonable nexus between the invasion and the job, *Cort* and *Bratt* view the test as balancing the invasion of privacy with the employer's need for the information. At the end of the day, whether the court weighs the factors or finds a connection between them, the relevant inquiry remains the same: How intrusive was the question/information and is the controversial information related or relevant to the job?

¹¹⁶*Pemberton v. Bethlehem Steel Corp.*, 66 Md. App. 133 (1986).

¹¹⁷*Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 576 (1976).

1. *Cort v. Bristol-Myers Co.*¹¹⁸: After determining that its Boston sales division was performing the worst, executives at Bristol-Myers sent questionnaires to each Boston district salesman with the instructions to answer completely and return the forms. The salesmen objected to certain questions as highly personal and offensive, and determined the questions as not related in any apparent way to their job performance. Each salesman returned the questionnaire but failed to give answers or gave frivolous answers to many questions. Every salesman who failed to answer the questions completely received a warning letter and was eventually fired. At the trial court, directed verdict was granted for Bristol-Myers on the salesmen's claims of invasion of privacy. The judge found that because the salesmen declined to provide any information, their privacy had not been invaded. "We are not concerned here with an employee who answered unreasonably intrusive personal questions under the threat of being discharged if he did not answer those questions."¹¹⁹ The Supreme Judicial Court of Massachusetts upheld the claim for dismissal, finding that most of the unanswered questions were relevant to the plaintiffs' job qualifications. However, the court claimed that if the questionnaire sought to obtain information in circumstances that constituted an "unreasonable, substantial or serious interference with his privacy,"¹²⁰ the discharge of an employee for failure to provide such information could contravene public policy and warrant the imposition of liability on the employer for the discharge. Essentially, if Bristol-Myers had no right to ask the questions that the salesmen declined to answer, then Bristol-Myers could be held liable for discharging the salesmen for their failure to answer.

"This opinion simply acknowledges that in the area of private employment there may be inquiries of a personal nature that are unreasonably intrusive and no business of the employer and that an employee may not be discharged with impunity for failure to answer such requests."¹²¹

The court did not go so far as to state that an employer would always be liable for releasing an employee for his refusal to answer questions not relevant to business purposes, but it did create a test to

¹¹⁸*Cort v. Bristol-Myers Co.*, 385 Mass. 300, 431 N.E.2d 908 (1981).

¹¹⁹ 385 Mass. 300, 303.

¹²⁰ *Id.* at 307.

help measure intrusions. The relevant test measures the nature of the intrusion, at least as to its reasonableness (but perhaps as well as to its substantiality and seriousness), and the nature of the employee's job is of some significance. "The information that a high level or confidential employee should reasonably be expected to disclose is broader in scope and more personal in nature than that which should be expected from an employee who mows grass or empties waste baskets."¹²²

2. ***Bratt v. International Business Machines Corp.***¹²³: *Bratt* further defines the balancing test identified in *Cort*. It explained that an "unreasonable interference with a right of privacy" occurs when the employee's right to keep information private outweighs the importance of the information in assessing the employee's work efficacy. *Bratt*, then, extended this same balancing test to two additional situations. These situations are determining when there has been an invasion of privacy resulting from: 1) an employer's disclosure of an employee's private information and 2) when the information disclosed about an employee is medical information from a physician.

3. ***Soroka v. Dayton Hudson Corp.***¹²⁴: The Dayton Hudson Corporation, who owns and operates Target Stores, required security officer applicants to take a psychological test. While they did not carry guns, the security officer's main job was to observe, apprehend, and arrest suspected shoplifters. The test was used to screen out applicants who were emotionally unstable, who may put customers or employees in jeopardy, or who would not take direction and follow Target procedures. This test was comprised of the MMPI and the California Psychological Inventory, both of which are tests that have been used to screen out emotionally unfit applicants for public safety positions. Yet, there were questions about an applicant's religious attitudes and sexual orientation. At the trial level, the court found that Target demonstrated a legitimate interest in psychologically screening applicants for security positions to

¹²¹ *Id.* at 307.

¹²² *Id.* at 308.

¹²³ *Bratt v. International Business Machines Corp.*, 392 Mass. 508, 467 N.E.2d 126 (1984).

¹²⁴ *Soroka v. Dayton Hudson Corp.*, 1 Cal.Rptr.2d 77 (1993).

minimize the potential danger to its customers and others. Finding Target's practice of administering this test to the applicants as reasonable, the court denied both parties' motions for summary adjudication.

On appeal, the court chose to apply the nexus requirement, using the lower federal standard to construe the state's right to privacy. The nexus requirement is that "[e]mployees may not be compelled to submit to a violation of their right to privacy unless a clear, direct nexus exists between the nature of the employee's duty and the nature of the violation."¹²⁵ Applying this test, the court found that Target had an unquestionable interest in employing emotionally stable persons as security officers. However, testing applicants about their religious beliefs and sexual orientation did not further this interest. At the end of the day, to pass the nexus-balancing requirement, a company must justify the invasion of privacy resulting from the use of the test through a compelling interest and the company must establish that the test serves a job-related purpose.

4. ***Johnson v. K Mart Corporation***¹²⁶: A group of 55 current and former employees of a K Mart warehouse sued for invasion of privacy and infliction of emotional distress stemming from the company's hiring of a security contractor whose employees passed themselves off as co-workers in order to gather information for K Mart. While the investigation was supposed to focus on K Mart's concerns of theft, sabotage, safety, and drug use, the undercover agents reported on many other subjects concerning the off-duty activities of the employees. These activities included: employee family matters, romantic interests/sex lives, future employment plans, complaints about K Mart, and personal and private concerns. The employees contended that K Mart invaded their privacy by intruding upon their seclusion; they did not challenge the effort to control theft and drugs, rather the collection of their private information.

This case was the first time that the state of Illinois expressly recognized a cause of action for the tort of invasion of privacy by intrusion upon seclusion. A successful cause of action for this requires that the plaintiff show: 1) an authorized intrusion or prying into the plaintiff's seclusion; 2) an intrusion that is

¹²⁵ *Id.* at 85.

offensive or objectionable to a reasonable person; 3) the matter upon which the intrusion occurs is private; and 4) the intrusion causes anguish and suffering. The Appellate Court found this tort to apply and held that enough material facts had been placed in issue to warrant a trial. Furthermore, the court focused on the deceptive nature of these acts and explained:

“A disclosure obtained through deception cannot be said to be a truly voluntary disclosure. Plaintiffs had a reasonable expectation that their conversations with ‘coworkers’ would remain private, at least to the extent that intimate life details would not be published to their employer.”¹²⁷

The court stressed the fact that deception had been used to garner the information, that no business purpose could be shown for the collection of that information, and that the agents were never instructed not to collect it even as their reports were continually submitted.

5. ***French v. United Parcel Service, INC.***¹²⁸: French, a UPS worker, took some of his fellow employees to a beer festival after completing a shift. One of the invited employees, Clark, was French’s supervisor and the other two were also in supervisory positions, but were lower in rank than the plaintiff. After the festival, the group spent several hours at the plaintiff’s home, where one member, Debutts, consumed alcoholic beverages and became intoxicated, emotionally volatile, and uncontrollable. French allowed Debutts to stay in his garage until he became sober. While he was alone in the garage, Debutts “lost control and went into a violent rage, causing injury to himself.”¹²⁹ French, along with the two other members of the group, found this employee lying in the garage bleeding. An ambulance was called and the employee was taken to a hospital and later released after twenty-four hours.

The plaintiff’s supervisor, Clark, pressed French to report this incident to his supervisors, but French refused to because he believed that the incident was none of UPS’s business. After additional pressing, French did relate the incident to his superiors. He was then put on leave pending an

¹²⁶*Johnson v. K Mart Corp.*, 311 Ill.App.3d 573, 723 N.E.2d 1192, 243 Ill.Dec. 591 (2000).

¹²⁷*Id.* at 579.

¹²⁸*French v. United Parcel Service, Inc.*, 2 F.Supp.2d 128 (1998).

investigation of the incident. During the next months, UPS personnel demanded that French meet with them to discuss the incident. At these meetings, French was “peppered with questions, brow-beaten about the incident, and otherwise shamed and made to feel as if his life outside work was important to his success and future with UPS.”¹³⁰ In addition, UPS repeatedly contacted the mental health professionals who were treating French for depression to determine his condition and prognosis for recovery. French was then demoted, but after returning to work, he resigned because of the humiliation he felt having to perform tasks he had not done in many years.

French alleged that UPS violated his right to privacy by insisting that he disclose details about an incident that occurred during off-work hours at his home, contacting his mental health doctors without consent, and penalizing him through involuntary leave and demotion for the off-work incident. The District Court held that an employer’s questioning of an employee about alleged drunkenness of a coworker at an employee’s home was not an invasion of privacy. The court explained that the Massachusetts’s right of privacy statute provides that “‘A person shall have a right against unreasonable, substantial or serious interference with his privacy.’ To constitute an invasion of privacy, the invasion must be both unreasonable *and* serious or substantial.”¹³¹ To this end, private acts under the Massachusetts Privacy Act are not necessarily those that are not public or not widely known. Rather, they are as *Bratt* defined, “required disclosure of facts about an individual that are of a *highly personal or intimate nature*.”¹³² The fact that a coworker drank in excess at French’s house is not a fact about French that qualifies under this standard. Furthermore, the facts of what happened in the incident were not private to French. Three other UPS employees were present at the event and were free to describe the incident. Clark, as French’s superior, may have owed UPS a duty to report what he had observed.

¹²⁹ *Id.* at 130.

¹³⁰ *Id.*

¹³¹ *Id.* at 130–31.

¹³² *Id.* at 131.

The court cited *Cort* and *Bratt* to explain that there are legitimate purposes for an employer to know the “personal” information of its employees, namely when the information bears upon the employee’s fitness for their employment responsibilities. In this context, the legitimate interest must be balanced against the seriousness of the intrusion on the employee’s privacy. In this case, UPS had a

“legitimate business reason for seeking information about the incident, including concerns about the soundness of judgment exercised by its supervisory employees in regard to alcohol abuse generally as well as in a particular setting where all participants were UPS employees.”¹³³

In this way, the court balanced the interests of the parties and came to the conclusion that there was not an actionable claim. In both *Johnson* and this case, the court looked to this evaluation to determine if there is an actionable invasion of privacy. However, this is in stark contrast to the *Johnson* case because UPS did not deceive in its method of obtaining the information. This case is also distinguishable because while *Johnson* had a reasonable expectation that their conversations would remain private, French had no such expectation to the events at his house. Furthermore, French’s expectation of privacy rested on the assumption that his off-duty activities did not affect his job. The court found that, unlike *Johnson*’s “reasonable expectation of privacy,” French’s mistaken evaluation of his job did not constitute an actionable invasion of privacy.

IV. Analogous Lines of Cases

As the previous cases have shown, “balancing pervades privacy law.”¹³⁴ The following cases are examples of when courts have applied these balancing tests to issues similar to GPS technology. In these cases the Fourth Amendment is used to show how courts will weigh specific privacy interests. Half the battle is proving that there is a privacy interest to protect. These cases are examples of privacy interests, where half the battle has already been won. They represent a trend in decisions; these are cases that have found that the privacy interest outweighs the “need to know.”

¹³³ *Id.*

¹³⁴ Craig M. Cornish & Monique A. Tuttle, *Privacy in the Workplace and in the Course of Litigation*, Chap. 9.9.6.

A. Supreme Court Cases

1. **Kyllo v. United States**—The *Kyllo* decision confronted the issue of the transformative nature of society. In *Kyllo*, the FBI used heat-sensing technology to discover whether the heat emanating from the walls and roof of a suspected marijuana grower’s house was sufficient to indicate the presence of the FBI high-intensity lights necessary for the plant’s indoor cultivation. To find the heat, the FBI employed a heat-sensing device, and it used the result of the high-tech search to obtain a warrant. Justice Scalia framed the question as: “What limits [are] there upon this power of technology to shrink the realm of guaranteed privacy?”¹³⁵ The court decided that basic constitutional protections do not disappear in the presence of a new technology. The *Kyllo* court said,

“We think that obtaining by sense-enhancing technology any information regarding the interior of the home could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area’ constitutes a search at least where the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.”¹³⁶

The *Kyllo* Court spelled out how the expectation of privacy can change when one is faced with a new technology. The expectation of privacy one has in public is not absolute. Yet, there are reasonable expectations of privacy when one is in a public place. The presence of technology can alter that expectation. For instance, if FBI agents stationed outside *Kyllo*’s house had noticed unusual patterns of melting snow on the roof and sides of the house and from those patterns deduced the presence or use of heat lamps, *Kyllo* could not have had a reasonable expectation of privacy.¹³⁷ Thus, deducing the presence of the marijuana-growing heat lamps from the snow patterns would have been acceptable. However, using a technological device to enhance their perception, enabling them to “see” things one would not expect to be visible in public, the FBI violated a reasonable expectation of privacy.

¹³⁵ *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

¹³⁶ *Id.* at 38.

¹³⁷ See White, *supra* note 23.

2. **United States v. Knotts**—In *Knotts*, the Supreme Court held that monitoring the signal of a beeper placed in a container of chemicals that was being transported to the owner’s cabin did not invade any legitimate expectation of privacy on the cabin owner’s part and, therefore, there was neither a “search” nor a “seizure” within the contemplation of the Fourth Amendment. The court justified this finding by stating that:

“Admittedly, because of the failure of the visual surveillance, the beeper enabled the law enforcement officials in this case to ascertain the ultimate resting place of the chloroform when they would not have been able to do so had they relied solely on their naked eyes. But scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise.”¹³⁸

Thus, in this case the court found a distinction between the sense enhancing technology used in *Kyllo* and that used in *Knotts*. The court explained that “Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.”¹³⁹ Furthermore, “beepers are merely a more effective means of observing what is already public.” To address the concerns that the police should not be able to track a person’s location, the court responded by quoting the Court of Appeals: ‘...a principal rationale for allowing warrantless tracking of beepers, particularly beepers in or on an auto, is that beepers are merely a more effective means of observing what is already public.’¹⁴⁰”

B. The California Cases

The California Supreme Court has been very progressive in the area of privacy law in the public sector. As a result, the California Constitution guarantees its citizens a right of privacy from both public and private invasions.

¹³⁸ *U.S. v. Knotts*, 103 S. Ct. 1081, 1087 (1983).

¹³⁹ *Id.* at 1086.

¹⁴⁰ *Id.* at 1086-87.

1. **Hill v. National Collegiate Athletic Association**-- In this case, student athletes filed a complaint alleging that the drug testing programs of intercollegiate athletic association violated their right of privacy. The court required the NCAA to demonstrate that: (1) the testing program relates to the purposes of the NCAA regulations which confer the benefit (participation in intercollegiate competition); (2) the utility of imposing the program manifestly outweighs any resulting impairment of the constitutional right; and (3) there are no less offensive alternatives.¹⁴¹ The court found that the NCAA had not satisfied any of these requirements and held that the drug testing was an invasion of privacy protected by the California Constitution.

2. **Shulman v. Group W. Productions**—In *Shulman*, the California Supreme Court held that an injured accident victim could reasonably expect that her conversations with her rescue nurse were not being electronically recorded through a small microphone placed on the nurse. This holding was largely influenced by California’s Invasion of Privacy Act, which prohibits the electronic communication recording of any “confidential communication” without the consent of all the parties to the communication.¹⁴² The California Penal Code §632 states that a

“ ‘confidential communication’ includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes ... any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded”¹⁴³

Essentially, this statute protects a party’s reasonable expectation of privacy in a conversation from any type of electronic recording.

In addition to the code, the court found that there was a reasonable expectation of privacy because the accident was removed from the view of the general public. Without the taping of the incident, the general public may have never viewed the accident. The court also reasoned that Ruth’s conversations

¹⁴¹ See *Hill v. Nat’l Collegiate Athletic Ass’n*, 273 Cal. Rptr. 402, 410 (1990).

¹⁴² *Shulman v. Group W. Prods., Inc.*, 18 Cal. 4th 200 at 234, (quoting Cal.Penal Code §632 West 2004).

¹⁴³ Cal. Penal Code §632 (West 2004).

were in the course of medical treatment, which is traditionally and legally considered a situation that has an expectation of privacy. The Invasion of Privacy Act, the location of the accident, and the conversation during medical treatment created enough evidence for the court to find that the reasonableness of the expectation of privacy was an issue of fact in this case.

3. **Sanders v. American Broadcasting Companies**-- In *Sanders*, a coworker and an undercover investigative reporter had a conversation at their place of work, which was taped. The plaintiff, Mark Sanders, discussed intensely private and personal information with the reporter. He “discussed his personal aspirations and beliefs and gave [the defendant] a psychic reading.”¹⁴⁴ The California Supreme Court held that Sanders could have a reasonable expectation of privacy in the workplace against the videotaping of his conversation, even though he lacked a reasonable expectation of privacy from the rest of the people in his office.

C. Government’s Use of GPS

The fact that the satellites used by GPS companies are owned and maintained by the government creates more complexity for the issue of GPS tracking in the workplace.

1. **State v. Jackson**--Washington State has case law that protects its citizens from having their locations tracked by the government. In *State v. Jackson*,¹⁴⁵ the court addressed the question of whether or not the government could use GPS tracking of an automobile to trail a suspect. *Jackson* decided that the installation of GPS devices for satellite tracking of a defendant's vehicle involved "search and seizure" and required a warrant. Unlike binoculars or a flashlight, the device did not merely augment the police officers' senses, but provided a technological substitute for traditional visual tracking and the possible intrusion into private affairs was quite extensive. Furthermore, state citizens have a right to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle, regardless of reduced privacy expectations due to advances in technology. The Washington Constitution

¹⁴⁴ *Sanders v. Am. Broad. Cos.*, 85 Cal.Rptr.2d 907 at 912 (1999).

¹⁴⁵ *State v. Jackson*, 76 P.3d 217 (Wash., 2003).

influenced this decision in a large part: “No person shall be disturbed in his private affairs, or his home invaded, without authority of law.”¹⁴⁶ While the court found that GPS tracking by the government requires a warrant, it did not hold for the plaintiff. The court held that there was no constitutional violation because the police in this case obtained valid warrants.

In the analysis, the Supreme Court of Washington classifies GPS tracking of an individual’s location as invasive when it writes:

“Moreover, the 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. In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles. The GPS tracking devices record all of these travels, and thus can provide a detailed picture of one's life.”¹⁴⁷

Here the Supreme Court of Washington clearly finds that it is an invasion of privacy for the government to track locations with GPS. While this decision is only applicable to police tracking of suspects with GPS, it could be applicable to any government tracking of individuals. Furthermore, this case makes location information a valid privacy interest; it establishes that courts have previously protected the public’s right to privacy under these circumstances.

2. ***Johnson v. State***--The Jackson decision justified its findings by referencing a Florida Court of Appeals case. In *Johnson v. State*,¹⁴⁸ the Florida Court of Appeals was faced with a similar issue under the Fourth Amendment when a tracking device was installed on an airplane. Officers had a warrant authorizing installation of a device “upon or under” the aircraft, but also installed an additional tracking device under a panel at the rear of the interior of the plane. The first device failed; the second worked. The court found

¹⁴⁶ West's RCWA Const. Art. 1, § 7.

¹⁴⁷ *State v. Jackson*, 76 P.3d 217, 262 (Wash., 2003).

that the installation of the second device was “tantamount to an illegal entry and beyond the scope of the warrant,” and suppressed evidence obtained through its use. While this is not the equivalent of the modern-day GPS tracking, the device had a similar function. It was a transponder or an electronic device, which responds to a signal from a radar station so that the radar station can locate and identify the aircraft.

3. ***People v. Oates***--The Supreme Court of Colorado considered a similar issue in *People v. Oates*.¹⁴⁹ In *Oates*, the court held that the warrantless placement of a beeper in a drum of chemicals allegedly used to manufacture drugs was an illegal search as to a defendant who had partially purchased and taken possession of the drum. In their decision, the court considered how location-tracking technology could invade an individual’s privacy.

“Whether an expectation of privacy is reasonable may be tested against the customs, values and common understandings that confer a sense of privacy upon many of our basic social activities. Government surveillance necessarily reduces this sense of privacy; many citizens may choose to curtail their freedom of action rather than risk exposure of their activities to government scrutiny.”¹⁵⁰

Thus, *Oates* classified location-tracking technology to be an invasion of privacy. However, the court went a step further and found that this invasion of privacy could potentially stop individuals from performing their everyday activities because of fear. The court characterized this as a threat to individual freedoms. Furthermore, the court found that “[k]nowing the movements of an item and its possessor may permit the government to reconstruct ‘a virtual mosaic of a person’s life,’¹⁵¹ including ones habits, habitats, and associates.”¹⁵²

4. ***People v. Lacey***—In a recent unpublished decision, the County Court of Nassau County of New York decided whether the fourth amendment protections extend to the installation of a GPS device. It held that the attachment of a GPS device requires a physical intrusion into an individual’s personal effects. The court found that the defendant did not have a legitimate expectation of privacy because he did not own the

¹⁴⁸ *Johnson v. State*, 492 So.2d 693, 694 (Fla.App. 5th Dist., 1986).

¹⁴⁹ *People v. Oates*, 698 P.2d 811 (Colo., 1985).

¹⁵⁰ *Id.* at 816.

¹⁵¹ *People v. Sporleder*, 666 P.2d 135, 142 (Colo.1983).

automobile on which the GPS was installed. However, *Oates* stated that, in the absence of exigent circumstances, the police should obtain a warrant prior to attaching a GPS device to an automobile.

“At this time, more than ever, individuals must be given the constitutional protections necessary to their continued unfettered freedom from a ‘big brother’ society. Other than in the most exigent circumstances, a person must feel secure that his or her every movement will not be tracked except upon a warrant based on probable cause establishing that such person has been or is about to commit a crime. Technology cannot abrogate our constitutional protections.”¹⁵³

Here the court clearly finds not only that there is a privacy interest, but that this interest is protected by the constitution.

In addition to the cases described in this section, there are other influential government surveillance cases that have weighed location-tracking technology against individual expectations of privacy. See: *U.S. v. Karo*, 468 U.S. 705, 104 S. Ct. 3296; *State v. Campbell*, 306 Or. 157, 759 P.2d 1040; *Osburn v. State*, 44 O.3d 523 (Or. 2002).

V. Secondary Sources

1. *GPS Invasion of Worker Privacy*

The Maryland Bar Journal has recently published an article called *GPS Invasion of Worker Privacy*¹⁵⁴, which directly tackles the issue of GPS and physical location employee tracking. Two forms of common technology are classified as geographic tracking: fencing and cell phones. Fencing is identified as a system that tells an employer the instant a vehicle enters or exits a geographic zone and how long it stays there. The Nextel i88s is a cellular phone that has a GPS chip, which allows managers to see their employee’s location plotted on a computerized map. This article attempts to advise employers on ways to effectively monitor employees without becoming liable for invasion of privacy. It explains that federal and state statutes prohibit certain electronic surveillances, such as eavesdropping on telephone calls, voice-mail, or emails, but these statutes do not apply to monitoring an employee’s location. The

¹⁵² *People v. Oates*, 698 P.2d 811, 817.

¹⁵³ *People v. Lacey*, No. 2463N/02 (N.Y. County Ct. Nassau County, May 6, 2004).

article hypothesizes that workers will turn to the common law tort of invasion of privacy in order to seek redress for psychological distress caused by the intrusion. In this way, the article finds that the *Pemberton v. Bethlehem Steel Corp.* case becomes relevant. Through this case, a company can monitor the off-duty location of its employees, as long as the surveillance is reasonable, unobtrusive, and for a job-related purpose. Unreasonable surveillance is defined as monitoring that a reasonable man would find to be “highly offensive.” This poses the question that is yet to be answered: What does a reasonable man consider to be “highly offensive?” The author of the article attempts to answer this question by advising his reader to balance the benefits of using surveillance outside the workplace against the chance of a lawsuit. Essentially, the employers are advised that electronic monitoring is risky because it could alienate the staff and cause litigation, but it could increase productivity and for that reason, employers should do a personal calculus to evaluate the situation.

Five steps are recommended to integrate electronic surveillance into the workplace. 1) Employers should present employees with a blueprint for using the technology, explaining what information will and will not be gathered. 2) Employers should make a policy public to the staff and retain a written record of the employees’ acknowledgment of the policy. 3) Companies should couple any location technology with some type of mobile work equipment, sending job-related data between the office and the worker’s home. This, effectively, keeps the employee on the job at all times and would lower the anxiety of a workforce suspicious of electronic surveillance. For example, an employer could send a computer to a worker’s home so that the worker could finish his task at his leisure. Then, the line between being off-hours and on-hours is blurred and GPS tracking becomes a greater possibility. 4) Employers should appreciate that employees will take care of personal needs on company time; this violation should not be overly punished. 5) Finally, any company that is going to physically track their employees should get legal advice, as this is an issue that is not settled and what is permitted in one set of circumstances may create liability in another.

¹⁵⁴ Murray Singerman, *GPS Invasion of Worker Privacy*, 37 Md. B.J. 54 (May/June 2004).

To show the application of these suggestions, the author gives two examples of companies attempting to integrate tracking devices into the workforce. The article details a successful integration of location technology into a business, which did not cause a workers' rebellion. A year after a utility fiasco, workers in California accepted an AVL system monitoring 625 city employees. The city union explained that the agency only wanted to track the employees to ensure uniform supervision and discipline. To show how much employees tend to cherish their privacy, the circumstances of a Midwestern utility use of geographical positioning technology is detailed as well. After spending \$1 million to track 700 service technicians with an AVL system, the union fought back. The union claimed that the AVL equipment exposed workers to harmful levels of radio waves. Fearful of a strike or lawsuit, the company decided that \$1 million was far cheaper than a union strike or litigation and withdrew the system after three months of use.

2. Privacy Rights, Public Policy, and the Employment Relationship

In the Ohio State Law Journal, Pauline T. Kim wrote *Privacy Rights, Public Policy, and the Employment Relationship*.¹⁵⁵ Kim finds that for the typical private sector employee, the only general source of legal protection from unjustified employer intrusions is the common law. She explains that invasion of privacy does offer protection against all manners of unreasonable intrusions on employee privacy, but the application is complicated by the conflicting right of the employer to terminate the relationship at-will. Kim focuses on this complication and argues that any meaningful protection of an employee's privacy requires a limitation of the employer's power to terminate at-will. The courts that have dealt with this issue have held that an employer may be held liable for the tort of invasion of privacy when he enters an employee's home without permission. However, when the employer gives advance notice of the intrusion, the tort loses weight. Thus, if the employee allows the company to invade his privacy, the company will claim that he consented to the intrusion. Conversely, if an employee objects to

¹⁵⁵ Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 Ohio St. L.J. 671 (1996).

the device, the strict application of the at-will doctrine would allow the employer to fire him. Additionally in this situation, common law tort would provide little to no relief.

Kim focuses on how an employee can use the common law tort system to insure his privacy. She explains that:

“The paradigm intrusion case occurs when someone enters a private space, such as a person’s home, hotel room, or hospital room without permission. Unlawful intrusions, however, need not be physical; what the common law tort seeks to protect is not merely space, but an individual’s ‘private affairs or concerns.’ Thus, it not only prohibits traditional forms of spying, such as binoculars to peer into windows of a home, but extends protection to private activities and conversations and certain types of sensitive information as well. In order to be actionable, the intrusion must be ‘highly offensive to a reasonable person.’”¹⁵⁶

Essentially, this defines what monitoring is allowed by a sliding scale of community norms. Furthermore, notice is an important factor of what society would consider as “highly intrusive.” The example paradigm shows how the *Katz* decision is integrated into the evaluation of electronic geographic position tracking, as the nature of the locations and notice are directly related to society’s “reasonable expectation of privacy.” The article continues this study by discussing different views on what is highly intrusive, the argument that employee privacy interferes with a free market, and privacy rights as public policy. At the end of the day, Kim claims that employees retain their “ordinary, socially established expectations of privacy in the workplace,” except when there is a waiver. Therefore, there must be justification for any invasion of privacy because there is a fear that the market may eventually induce a form of self-violation. She essentially argues that common law privacy rights should be recognized as a limitation on the traditional prerogative of the employer to terminate at-will.

3. ***Privacy Issues in the Private-Sector Workplace: Protection From Electronic Surveillance and the Emerging “Privacy Gap”***

¹⁵⁶ *Id.* at 689.

In the Southern California Law Review, David Neil King wrote an article entitled *Privacy Issues in the Privacy-Sector Workplace: Protection from Electronic Surveillance and the Emerging “Privacy Gap.”*¹⁵⁷ In this article, the “reasonable expectation of privacy” test is explored in the context of invasion of privacy through intrusion into seclusion. King explains that what qualifies as an intrusion may have something to do with the nature of the prying and it must be something that would be objectionable to a reasonable person. He summarizes:

“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 . . .privacy, if the intrusion would be highly offensive to a reasonable person. There are no absolute defenses to this tort.”¹⁵⁸

However, the application of this rule is problematic when applied to electronic monitoring because it is hard to define an employee’s “reasonable expectation of privacy” and then balance the employer’s interest against this expectation. The importance of the “reasonable expectation of privacy” derives from the requirement that the monitoring must have intruded on something private. This standard would hypothetically provide an objective way to measure the appropriate level of privacy that a person should reasonably expect. Then, in the second analysis, the employee’s privacy interest is balanced against the employer’s interest in running a business. King uses this article to explain how these two tests have actually merged and left plaintiffs without an appropriate legal remedy.

“In the area of intentional tort, however, the objectively-reasonable-expectation test has taken a back seat to employers’ interests. Stated differently, the court may look to the employer’s interests to determine whether employees are actually asserting something they have a right to keep private.”¹⁵⁹

¹⁵⁷ David Neil King, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging “Privacy Gap”*, 67 S. Cal. L. Rev. 441 (1994).

¹⁵⁸ *Id.* at 459.

¹⁵⁹ *Id.* at 460.

In this way, King claims that the reasonable expectation test is dependent on the type of job and employer rather than the level of invasion. As a result, an employee could have an individual “reasonable expectation of privacy” but no right to keep the matters involved private. Thus, there is a gap between the methods an employer may use to monitor an employee and the protection afforded to the employee’s expectation of privacy. Yet, this gap is necessary for employers to have a legal means of monitoring their employees. King finds that the most efficient gap would be the least intrusive monitoring techniques possible that still yield valuable information about employee production levels or other work related information.

4. *Invasion of Privacy: Refocusing the Tort in Private Sector Employment*

An article in the DePaul Business Law Journal entitled *Invasion of Privacy: Refocusing the Tort in Private Sector Employment*¹⁶⁰ sheds more light on *Johnson’s* tort of invasion of privacy or seclusion. It explains that to be actionable, courts require the intrusion to be unreasonable. Judicial decisions often turn on the place of the intrusion.

“For example, intrusion upon someone in a public place is generally not deemed actionable. However, intrusion into the confines of a person’s home leads to a different result. When the intrusion, though job-related, occurs in the home or other private confines, the common law affords great protection to the employee. Yet when the intrusion occurs at the work site, common law does not afford as much protection.”¹⁶¹

The article explains this distinction through the basis for greater protection of privacy in the home, or outside the workplace. The law generally accords to individuals supreme rights of control over what is known to occur in their dwelling. However, the law accords to employers the supreme rights of control over the workplace. Thus, the common law recognizes an underlying legal right to control what others know about a person depending on the location of the intrusion.

¹⁶⁰ John D. Blackburn, *Invasion of Privacy: Refocusing the Tort in Private Sector Employment*, 6 DePaul Bus. L.J. 41 (1993).

¹⁶¹ *Id.* at 52-3.

This article also proposes a model that is similar to the balancing test applied in the earlier cases. Through the analysis of several cases, the article introduces a standard for the private sector that injects a requirement of reasonable suspicion into the determination.

“Under this proposed model, a court could look to constitutional law to determine if a right to control personal information exists. However, a court would use the qualified privilege to determine if the right is overcome by job related reasons justifying the employer’s conduct. Application of the qualified privilege results in a balancing of a constitutional framework for determining the scope of the plaintiff’s privacy right....”¹⁶²

The article suggests that the courts and legislation are attempting to protect a worker’s right to control what is known about him or her. However, it also suggests that the focus has not always been clear when dealing with invasion of privacy cases in the employment setting. The model proposed by this article has the advantage of accurately directing focus on protecting an employee’s right to control what is known about him or her from unreasonable interference. It provides a method for balancing the relative interests of the employer and employee to determine when an employee’s privacy interest has been interfered with unreasonably.

¹⁶² *Id.* at 67.

VI. Conclusion

GPS tracking is often simplified into tracking the real time location of a person; many do not associate it with a great invasion of privacy. One might think that it does not matter if their employer knows that he goes to Starbucks every morning before work or that they spend Sundays at his girlfriend's house. This line of thinking misses a larger point. If someone has the ability to know the real time location of a person around the clock, they are able to create a mosaic of that person's life. They learn everything about that person, much of which is highly personal and private in nature.

To a greater extent, when an employee knows that his boss watches his day-to-day activities, he might think twice before he takes part in certain activities. For example, if one's boss was a vigilant Republican, an employee might choose not to go to the Democratic National Convention. Tracking location affects autonomy. Matthew Finkin has written: "An axial principle which the right to privacy turns on is individual autonomy, a freedom from control or domination."¹⁶³ As technology evolves, this form of invasion of privacy could grow to control and dominate the public in dangerous ways. According to Moore's law, computing power doubles every eighteen months. Dan Farmer and Charles Mann recently described the implications of this theory on the ability to monitor individuals: "By 2023, large organizations will be able to devote the equivalent of a contemporary PC to monitoring every single one of the 330 million people who will then be living in the United States."¹⁶⁴

The potential location-tracking capability of future technologies is limitless. It is essential that the public understand how the technologies work and realize how they invade their privacy. The National Workrights Institute has and will continue to educate the public on the issues of GPS tracking in the workplace and advocate for the protection of workers' privacy rights from new and invasive technologies. We will be happy to work with you to address these new challenges as they arise.

¹⁶³ Matthew W. Finkin, *Employee Privacy, in Comparative Labor Law and Industrial Relations in Industrialized Market Economies* 209 (R. Blaupain & C. Engles eds., 6th ed. 1998).

BIBLIOGRAPHY

Aaron Reneger, *Satellite Tracking and the Right to Privacy*, 53 Hastings L.J. 549 (January 2002).
Amy Harmon, *Lost? Hiding? Your Cellphone Is Keeping Tabs*, available at <http://www.nytimes.com/2003/12/21/technology/21WATC.html> (Dec. 21, 2003).

Arik Hesseldahl, *War Highlights Role of GPS – Is Business Watching?*, available at http://www.mobileinfo.com/News_2003/Issue13/GPS_war.htm (last modified Apr. 16, 2003).

Betsy Stark, *Every Step You Take... Companies Using Tracking Devices to Monitor Employees*, available at http://abcnews.go.com/sections/wnt/WorldNewsTonight/wnt010104_workplace_tracking_feature.html (Jan. 4, 2001).

Bratt v. International Business Machines Corp., 392 Mass. 508, 467 N.E.2d 126 (1984).

Brendan I. Koerner, *Dial 'P' for Paranoid*, available at <http://www.villagevoice.com/issues/0221/koerner.php> (May 28, 2002).

Brendan I. Koerner, *Your Cellphone Is a Homing Device*, available at http://www.legalaffairs.org/issues/July-August-2003/feature_koerner_julaug03.html (Jul. 2003).

Cal. Penal Code §632 (West 2004).

Cathy Kightlinger, *Schools Looking to the Skies to Track Buses*, available at <http://www.indystar.com/articles/8/135547-9318-P.html> (Apr. 6, 2004).

Charles Forelle, *Big Brother Is Really Watching You*, available at <http://www.ocnus.net/cgi-bin/exec/view.cgi?archive=45&num=11841> (May 14, 2004).

Cheryl Buswell-Robinson, *Tracking Devices Anger Nurses*, available at <http://www.labornotes.org/archives/1999/0599/0599b.html> (May 1999).

City of Chula Vista, *Public Works – Operations*, available at http://www.chulavistaca.gov/City_Services/Community_Services/Public_Works_Operations/Admin/street_sweep.asp (last visited Aug. 2, 2004).

Cort v. Bristol-Myers Cos., 385 Mass. 300, 431 N.E.2d 908 (1981).

Craig M. Cornish & Monique A. Tuttle, *Privacy in the Workplace and in the Course of Litigation*, Chap. 9.9.6.

Daniel R. Sovocool, *GPS Update: The FCC Sets the Table for GPS Location Technology in Wireless Phones*, available at http://www.thelenreid.com/articles/article/art_57_idx.htm (last visited July 19, 2004).

Darren Griffin, *How Does the Global Positioning System (GPS) Work?*, available at <http://www.pocketgps.co.uk/howgpsworks.php> (Sept. 5, 2002).

¹⁶⁴ White, *supra* note 23.

Dave Lagergren, *Answers to Commonly Asked Questions About GPS/AVL Solutions*, at http://www.ccgroupp.com/gps_avl_faqs.htm (last modified May 27, 2004).

David Neil King, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap"*, 67 S. Cal. L. Rev. 441 (1994).

Dibya Sarkar, *Local Governments Use GIS*, available at <http://www.fcw.com/geb/articles/2003/1208/web-gis-12-11-03.asp> (Dec. 11, 2003).

Federal Communications Commission, *Enhanced 911*, at <http://www.fcc.gov/911/enhanced/> (last modified Mar. 10, 2004).

FleetAlert Vehicle Tracking System, available at <http://www.wirelesstelematics.com/products/fleetalert.html> (last visited July 21, 2004).

Frank James, *GPS Grows as Tool to Spy at Home, Work*, available at <http://www.chicagotribune.com/technology/chi-0302110306feb11,1,7768625.story> (Feb. 11, 2003).

French v. United Parcel Service, Inc., 2 F.Supp.2d 128 (1998).

Frequently Asked Questions, at <http://www.xora.com/timetrack/faq.html> (2004).

Grant Buckler, *GPS Tracking Becomes More Affordable for Small Business*, available at <http://www.theglobeandmail.com/servlet/ArticleNews/TPPrint/LAC/20040624/TWGPS24/TPTechnology/?mainhub=GT> (June 24, 2004).

Hill v. Nat'l Collegiate Athletic Ass'n, 273 Cal. Rptr. 402, 410 (1990).

<http://www.futureroads.com/trac2me/>.

Immanuel Kant, *General Introduction to the Metaphysics of Morals*, in GREAT BOOKS OF THE WESTERN WORLD, 275 (Robert Maynard Hutchins. Ed. And W. Hastie, trans., 1952).

Implementation of 911 Act, Fourth Report and Order and Third Notice of Proposed Rulemaking, 15 F.C.C.R. 17079, para. 1, 20 Comm. Reg. (P & F) 489 (2000).

James C. White, *People, Not Places: A Policy Framework for Analyzing Location Privacy Issues*, available at <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf> (2003).

Jane Applegate, *Are Your Employees Costing You?*, available at <http://www.entrepreneur.com/article/0,4621,289593,00.html> (May 17, 2001).

Jeffrey Selinger, *Protecting the Cellphone User's Right to Hide*, available at <http://www.nytimes.com/2004/02/05/technology/circuits/05next.html?ex=1086926400&en=77b53131ef4d6527&ei=5070> (Feb. 5, 2004).

John Canoni, *Employers Are Using Location Awareness Technology to Keep Track of Their Employees*, at http://www.nixonpeabody.com/publications_detail3.asp?Type=P&PAID=4&ID=486&Hot= (Jan. 8, 2004).

John D. Blackburn, *Invasion of Privacy: Refocusing the Tort in Private Sector Employment*, 6 DePaul Bus. L.J. 41 (1993).

Johnson v. K Mart Corp., 311 Ill.App.3d 573, 723 N.E.2d 1192, 243 Ill.Dec. 591 (2000).

Johnson v. State, 492 So.2d 693,694 (Fla.App. 5 Dist., 1986).

Judy Muller, *Worker Whereabouts: California City Monitors Employees Via Satellite Technology*, at http://www.abcnews.go.com/sections/wnt/SciTech/gps_employees_040221.html (Feb. 21, 2004).

Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 576 (1976).

Kevin Brown, *Wayne Uses Satellite Maps to Fix Roads*, available at <http://www.detnews.com/2004/wayne/0402/16/c04-64235.htm> (Feb. 15, 2004).

Kyllo v. United States, 533 U.S. 27, 34 (2001).

Lauren Spiers, *Routing & Tracking*, available at http://www.atroad.com/corp/presscenter/downloads/lawn_landscape_1103.pdf (Nov. 2003).

Matthew W. Finkin, *Employee Privacy*, in *Comparative Labor Law and Industrial Relations in Industrialized Market Economies* 209 (R. Blaupain & C. Engles eds., 6th ed. 1998).

Murray Singerman, *GPS Invasion of Worker Privacy*, 37 Md. B.J. 54 (May/June 2004).

Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 Ohio St. L.J. 671 (1996).

Pemberton v. Bethlehem Steel Corp. 66 Md. App. 133 (1986).

People v. Lacey, No. 2463N/02 (N.Y. County Ct. Nassau County, May 6, 2004).

People v. Oates, 698 P.2d 811 (Colo., 1985)

People v. Sporleder, 666 P.2d 135,142 (Colo.1983).

Point of View: What is the Status of Office of the County Surveyor Today?, available at http://www.pobonline.com/CDA/ArticleInformation/PointOfView_Item/0,2432,87809,00.html (last modified Nov. 18, 2002).

Richard B. Langley, *In Simple Terms, How Does GPS Work?*, available at <http://gge.unb.ca/Resources/HowDoesGPSWork.html> (last modified Mar. 27, 2003).

Samsung Releases GPS Phone, at <http://slashdot.org/articles/01/10/10/2115236.shtml> (Oct. 10, 2001).

Sanders v. Am. Broad. Cos., 85 Cal.Rptr.2d 907 at 912 (1999).

Scott Mace, *Track Stars*, available at http://www.nurseweek.com/news/features/03-07/ortracker_web.asp (July 3, 2003).

Shulman v. Group W. Prods., Inc., 18 Cal.4th 200 at 234, (quoting Cal.Penal Code §632 West 2004).

Soroka v. Dayton Hudson Corp. 1 Cal.Rptr.2d 77 (1993).

Stacy A. Teicher, *The Boss's Big Eye in the Sky: Companies Turn to Satellite Tracking Tech to Watch Workers*, available at

http://abcnews.go.com/sections/scitech/US/GPS_spies_workers_CSM_031223.html (Dec. 23, 2003).

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

Susan Trossman, *Tool or Weapon? Nurses Talk About Being 'Tracked'*, available at

<http://www.nursingworld.org/tan/01marapr/tracked.htm> (Apr. 2001).

Telephone Interview with Wescom Products, Inc. (Aug. 2, 2004).

Tony Hallett, *Mobile-Tracking Start-Up Sees "Huge Rise" in Users*, available at

<http://networks.silicon.com/mobile/talkback.htm?PROCESS=show&ID=20023079&AT=39120068-39024665t-40000018c> (2004).

U.S. Public Stirred (Not Shaken) by Future Mobile Phone Possibilities, available at

http://www.letstalk.com/company/release_022200.htm?depId=0&pgId=0 (Feb. 22, 2000).

U.S. v. Knotts, 103 S. Ct. 1081, 1087 (1983)

Wescom Products, Inc., *Intelligent Locator: A System Smart Enough to Find Anyone Anytime Anywhere*, available at <http://www.nursecall.com/Intelligent%20Locator%20System.htm> (last modified June 8, 2004).

West's RCWA Const. Art. 1, § 7.

Where Am I?, at http://www.blog.fastcompany.com/archives/2003/09/12/where_am_i.html (Sept. 12, 2003).

Your Cell Phone Is Probably a GPS Tracking Device, at <http://www.interesting-people.org/archives/interesting-people/200308/msg00024.html> (Aug. 6, 2003).