## Bupple FONA PLOYE EM Ksia **NG TECHNOL** S

Telenia

Urstulin

too.

Lasy

Mszczonowska 409

Haletan

100

Ausie

6

INSKID

10

Mar

3

415

Slesine

402

AN ANOS

Bhwing

ieniec



You sent your employee to the post office, but the employee has not returned in several hours. Has there been an accident? Is the employee at home taking a nap on your time? Do you ever wish that you could track the location of your employees to determine whether they are performing the services for which you are paying them? Tracking is even more important when the employee is on the road for most of the day. Route sales staff, cab drivers and similar workers who drive for a living have traditionally been immune from the watchful eye of employers.

The problem is that employees do not like to be watched. As a result, the interest of the employer in effectively operating a business must be gauged against any privacy rights of the employee.

Published reports show that few employers are currently using GPS technology to track employees. Only five percent use GPS to track cell phones, eight percent use it to track company vehicles and eight percent use it to monitor employee identification badges or data cards.<sup>1</sup> Some companies are using RFID employ Smartcard technology to regulate entering and leaving the premises. According to a 2005 American Management Association "Electronic Monitoring and Surveillance Survey," 53 percent of employers use Smart Card technology in the workplace.

#### **Global Position Systems**

Global position system (GPS) monitoring makes real time position tracking possible and is an effective way to monitor and track company owned vehicles and hence employees. As one of the newest means of tracking employees, most of this article will focus on this technology.

GPS is helpful to employers who wish to monitor employees for a variety of reasons, including investigations, compliance with governmental regulations and adherence to company policy. The safety of the employee is also an often over looked reason for monitoring the location of company owned vehicles.

GPS provides a mechanism for ascertaining whether an employee is actually performing the job. For example, in the 2004 *Oman v. Davis School District* case, a Utah school district was concerned that an employee who worked for the district, but also owned an electrical contracting business, was leaving the school job during the day to perform electrical contracting work. GPS



NELSON ADRIAN BUSH is intellectual property counsel, Enterprise Solution. Fastman Kodak Company. Blish is past president of the Western New York Chapter of ACC and a captain, USN (ret). He is the author of Ishmael's Son, published by The Glencannon Press, and The Taking of the King, published by Penguin Books. He is currently working on his third novel, Silent Terror. He can be contacted at nelson.blish@kodak.com.



SHARON P. STILLER is a partner in the law firm of Boylan Brown Code Vigdor & Wilson LLP, a Primerus law firm, where she chairs the firm's employment practice group. Stiller is a fellow of the College of Labor and Employment Lawyers, and is the author of Fmployment Law in New York (West Group 2001) and a co-author with James E Metzler, Esq. of Expert Witnesses: Employment Cases. She can be contacted at sstiller@ boylanbrown.com.

is an ideal solution to investigate this type of concern, and to determine whether employees are going to assigned locations and doing what they report they are doing.

In another case, a comparison of a telephone technician's job log with a GPS tracking system installed on his truck, revealed nearly 30 times when the employee's records indicated that he was at a jobsite, but the GPS tracking system record showed he was actually at home. Needless to say, he was terminated for falsifying company records, misusing company time and property, and was later denied unemployment benefits in the 2007 *Perz v. Review Board of the Indiana Dept. of Workforce Development* case.

This technology also enables employers to determine if employees are complying with governmental regulations such as taking required breaks and not driving more hours than allowed.<sup>2</sup> This can be important in a number of industries, for example, the trucking industry and mass transit where the lives of passengers are at stake.

GPS is one of a number of technological innovations that enable employers to monitor individuals and is among the less intrusive. GPS relies upon reception of satellite signals by a ground receiver and computation of location of the receiver by its relation to the satellites. The location is compared to a digitized map, and presented for display on a LCD screen transmitted to a remote location, or both.

These sophisticated location devices may be mounted in automobiles, cell phones or other objects. Snowplow drivers in Massachusetts, for example, must carry GPS-equipped cell phones. UPS has distributed thousands

of handheld computers to its employees, each equipped with a GPS receiver. These uses increase the efficiency of operation of the business, but may also be used to monitor the activity of the employee.

Employees have the option to avoid off-duty monitoring by not using the company issued device containing the cell ID. Thus, an employee who is off-duty can choose not to use an employer provided cell phone when not at work. This would of course, alleviate some of the employee's privacy concerns.

#### **Other Monitoring Devices**

Other location monitoring devices include video surveillance cameras, RFID (Radio Frequency Identification) tags and cell identification and location technology.

Video surveillance has the potential of being used to track the actions of employees. The law on video surveillance is similar to the law on internet and email monitoring, which is well established. For video surveillance to be permissible, two questions arise: first, whether it is a public or private place and second, whether there is a reasonable expectation of privacy.<sup>3</sup> Often, advising employees of the fact of video surveillance discounts any claim of a reasonable expectation of privacy.

Some states such as New York, California and Rhode Island have statutes that regulate where video surveillance can occur. New York's statute, for example, prohibits employers from using video surveillance in a restroom, locker room or room designated by an employer for employees to change their clothes, unless authorized by court order. N.Y. Lab. Law § 203-c. However, where no such statute exists video surveillance in these types of areas is not prohibited.<sup>4</sup>

Cell IDs enable a network-based system to locate a cell phone. Being able to locate cell phones has such salutary purposes as enabling a taxi company to locate the closest taxi. It also has the potential to track employees. There is also a safety aspect to this capability. For example, in December 2006, a search for a lost Oregon family was aided by the "ping" from a cellular phone system. The fact that a text message had at least been partially delivered enabled trackers to locate the wife and children.

RFID is a generic term for technologies using radio waves to automatically identify individual items. An RFID system interrogates an item by transmitting a radio frequency signal, which is received by a "tag" on the item, and causes the tag to transmit a return signal with information about the identity of the item. Tags may be in the form of microchips, either active or passive, on the item.

Whether RFID tags impact privacy is debatable.<sup>5</sup> Because of capacity for storage of the data and compilation of databases, however, tracking individuals is possible, whereas GPS, at least in its most common form, can only trace the location of the vehicles driven by people. Note, however, that newer GPS cell phones, perhaps provided by the employer, may be used to track the location of the phone and hence the employee.

RFID tags on personal cards may be used to grant or deny employees access to different parts of the employer's premises. This information may be recorded and thus used to track movement of the employee. Another use of RFID tags would be to tag the company's assets, thereby enabling the employer to use a reader that would read both the assets' and the transporting employee's RFID tags. A Rand Corpo-

nericans with Disabilities Act + Sarbanes Oxley + Green Marketing + Distressed Commercial Real Estate + Obama Administration and the Environment + Controlling Costs + Corporate curities Law Update + International Staffing + Doing Business in Ontario + Family Medical Leave Act + Foreign Corrupt Practices Act + Ethics Super Session + Anti-Money Launderin undatory Disclosure + Reviewing and Negotiating Contracts + Discovery + Americans with Disabilities Act + Sarbanes Oxley + Green Marketing + Distressed Commercial Real Estate + Oba ministration and the Environment + Controlling Costs + Corporate and Securities Law Update + International Staffing + Doing Business in Ontario + Family Medical Leave Act + Fore rrupt Practices Act + Ethics Super Session + Anti-Money Laundering + Mandatory Disclosure + Reviewing and Negotiating Contracts + Discovery + Americans with Disabilities Act + Sarba ley + Green Marketing + Distressed Commercial Real Estate + Obama Administration and the Environment + Controlling Costs + Corporate and Securities Law Update + International Staffing obing Business in Ontario + Family Medical Leave Act + Foreign Corrupt Practices Act + Ethics Super Session + Anti-Money Laundering + Mandatory Disclosure + Reviewing and Negotiating tracts + corporate and Securities Law Update + International Staffing + Doing Business in Ontario + Family Medical Leave Act + Foreign Corrupt Practices Act + Ethics Super Session + A mery Laundering + Mandatory Disclosure + Reviewing and Negotiating Contracts + cDiscovery + Americans with Disabilities Act + Sarbane Soley + Green Marketing + Distressed Commer al Estate + Obama Administration and the Environment + Controlling Costs + Corporate and Securities Law Update + International Staffing + Doing Business in Ontario + Family Medical Leave Act + Foreign Corrupt Practices Act + Ethics Super Session + Anti-Money Laundering + Mandatory Disclosure + Reviewing and Negotiating Contracts + cDiscovery + Americans with Disabilities Act + Sarban Oxley + Green Marketing + Distee

rities Law Update • International Statting • Doing Business in Ontario • Family Medical Leave Act • Foreign Corrupt Practices Act • Ethics Super Session • Anti-Money Launderin latory Disclosure • Reviewing and Negotiating Contracts • eDiscovery • Americans with Disabilities Act • Sarbanes Oxley • Green Marketing • Distressed Commercial Real Estate • Oba inistration and the Environment • Controlling Costs • Corporate and Securities Law Update • International Staffing • Doing Business in Ontario • Family Medical Leave Act • Fore internation and the Environment • Controlling Costs • Corporate and Securities Law Update • International Staffing • Doing Business in Ontario • Family Medical Leave Act • Fore internation and the Environment • Controlling Costs • Corporate and Securities Law Update • International Staffing • Doing Business in Ontario • Family Medical Leave Act • Fore internation and the Environment • Controlling Costs • Corporate and Securities Law Update • International Staffing • Doing Business in Ontario • Family Medical Leave Act • Sarba international Staffing • Contracts • eDiscovery • Americans with Disabilities Act • Sarba

## Get CLE Credits Without Leaving Your Desk!

You need a source for fast, cost-effective information on the latest developments affecting your in-house practice. ACC Webcasts for CLE credit are your answer. Live webcasts are offered weekly and dozens are available on-demand.

Register for ACC Webcasts at webcasts.acc.com. To sponsor an ACC Webcast, contact accwebcasts@acc.com. [Education - Knowledge and training programs by and for in-house counsel.]



## While employers **are willing to videotape** employees or monitor their emails, employers are often **adverse to "tracking"** employees through **GPS.**

ration study found that most companies using RFID technology linked it to other databases, that the information was retained indefinitely and that the companies lacked auditing procedures to assure that the information was accurate.<sup>6</sup>

An Ohio surveillance company, CityWatcher.com, announced in a February 12, 2006, *The Financial Times* article that it had embedded RFID tags in two of its employees, with the employees' permission. CityWatchers' CEO, Sean Darks, explained: "We wanted not only to improve security for highly secure areas, but to do so with the next generation of product that would integrate with our existing system. The VeriChip was able to accomplish that goal." Darks noted the convenience of the chip being embedded in his arm. "Right now, I cannot find my car keys, but I have my chip," he said.

## Top Ten Pointers for Companies Considering Installing Monitoring Devices

- 1. Before installing monitoring devices, decide what you will do with the results. If you won't do anything with the results, don't bother with the device.
- 2. Determine whether your state has any restrictions on monitoring.
- 3. If the company is unionized, determine if monitoring is prohibited by the union contract.
- 4. If you choose to install monitoring devices, develop a policy.
- 5. Build privacy safeguards into your policy.
- 6. Disseminate the policy and update it each year.
- 7. Explain the purpose of monitoring to employees and how it impacts productivity and profitability.
- 8. Determine whether you will agree to any self-imposed restrictions on monitoring, such as agreeing not to discipline based solely on monitoring.
- Assure that monitoring is not applied in a discriminatory manner.
- 10. Continue to monitor updates in the technology that you are using.

Employees at CityWatchers have to swipe chips embedded under their skin past a detector to enter the facility. The tiny microchips do not contain any personal information other than the person's identity. Entering a location with the microchip implanted is similar to swiping a badge or card at the door. It tracks information about when a person entered or exited from a particular location. While some might liken it to the chip implanted in dogs so that they're not lost, the benefit is that employees do not have to remember ID cards, and timekeeping is accurate. When the person enters or leaves the employer's premises, the activity is simultaneously noted.

Not everyone is as excited about microchips as CEO Darks. In fact, the Smart Card Alliance, a nonprofit association composed mostly of high-tech firms and government agencies, has disavowed microchips for tracking employees. The organization said that microchips are "not the appropriate technology for securing human identification systems."

Nonetheless, as reported on MSNBC in 2004, the attorney general in Mexico required 160 members of his staff to have RFID chips inserted in their bodies so that their movements could be tracked. According to VeriChip, the company that makes the technology, as of 2006, approximately 2,000 people worldwide have had the chip embedded.<sup>7</sup>

Although the FDA approved implanting chips in 2004, there is now concern that the chips can be hacked, and that they may cause fast-growing malignant tumors in lab animals.<sup>8</sup> On the positive side, although not the subject of this article, an imbedded microchip may be used to store an individual's entire medical record, which may be invaluable if the person is brought to a medical facility in an unconscious state.

Another interesting method of monitoring employees, including those who work at home, is through webcams.<sup>9</sup> A light on the webcam, indicating it is activated, should meet the notice requirements with respect to privacy issues along with explicit company policy notification. Monitoring the computer activity of the employee, although working from home, would probably also be acceptable.

#### **Legal Issues Involved with Monitoring Through GPS** *Privacy Rights*

While employers are willing to videotape employees or monitor their emails, employers are often adverse to "tracking" employees through GPS. Perhaps that is because GPS tracking seems more intrusive or merely because it is a newer technology and the case law on the subject is in its infancy.

Courts generally hold that there is no reasonable expectation of privacy in the workplace of a private employer.<sup>10</sup> In addition, there is no reasonable expectation of privacy in an employer-owned vehicle. This concept stems from Supreme Court cases in the 1980s. As long ago as 1983 in *US v. Knotts*, the Supreme Court held that the installation of a tracking device in a drum of chloroform did not invade the defendant's legitimate expectation of privacy and therefore, was not a "search" or "seizure" within the meaning of the Fourth Amendment. As a result, courts have ruled that a search warrant was not required to install GPS on a vehicle, even by the police.<sup>11</sup>

"[N]othing in the Fourth Amendment prohibits the police from using science and technology to enhance or augment their ability to survey that which is already public. Inasmuch as constant surveillance by police officers of defendant's vehicle in plain view would have revealed the same information and been just as intrusive, and no warrant would have been necessary to do so, the use of the GPS device did not infringe on any reasonable expectation of privacy and did not violate defendant's Fourth Amendment protections."

Two courts disagreed. The Supreme Court of Oregon held in 1988 that use of a radio receiver to track a criminal suspect was a search within the meaning of the state's constitution, and therefore, a warrant was required. A 1988 Oregon Supreme Court case *State v. Campbell*, found holding that the covert attachment of a beeper or tracking device by police onto the exterior of an automobile constitutes a "search" under Oregon's Constitution.). On appeal, the Oregon Supreme Court held that the value to be protected was the right to privacy. Unlike simply viewing a vehicle, the court held, GPS tracking significantly limits freedom from scrutiny.

Similarly, the Supreme Court of Washington in the 2003 case *State v. Jackson* concluded that GPS tracking opens the door to extraordinary intrusion by the government. Even though the case was grisly — a murder case, where GPS led the police to the remote location where a father had buried the daughter he had murdered — the Court found that a warrant was required.

In employment-related cases, courts have ruled that use of a tracking device on a company car does not constitute a sufficient intrusion upon the employee's privacy to raise a claim, since it reveals no more than highly public information about the employer's vehicle's location as in the 2005 *Elgin v. St. Louis Coca-Cola Bottling Co.* case.

In a broader challenge to GPS requirements, a



## Straight from the top.

ACC's CLO Perspectives bring the insights of in-house leaders straight to you. See how GCs of the biggest companies deal with pressing issues and learn about the practices and management strategies they've established. [Networking - Unmatched opportunities to connect with the in-house community.]



To learn more visit www.acc.com/clo.

federal class action lawsuit was brought to challenge a New York City regulation requiring the installation in all licensed taxicabs of certain electronic equipment, including GPS systems. The plaintiffs in the 2007 case *Alexandre v. NYC Taxi and Limousine Commission*, claimed that this would substantially invade their privacy rights and be a financial burden, resulting in a government taking of their property rights in their taxicabs and the routes that they travelled. The court denied the requested injunction, ruling that the plaintiffs' claims to a privacy interest in the cabs and routes were not supported by law, and that requiring GPS served a legitimate governmental purpose. Ultimately, the lawsuit was settled and withdrawn.

#### Fourth Amendment

A Fourth Amendment analysis is inapplicable to private employers. Moreover, under the Fourth Amendment, the courts have held that the government can conduct warrantless searches of constitutionally private information and places if it does so with unenhanced human senses or sense-enhancing technologies in widespread use.<sup>12</sup>

#### Statutory Protections

There is no federal statute regulating location privacy, although one was proposed as early as 2001.<sup>15</sup> In 2004, an attempt to regulate RFIDs, the Opt Out of ID Chips Act [H.R. 4673, 108<sup>th</sup> Cong. (2004)], died in the House of Representatives.

## ACC Extras on...Technology and Employees

#### ACC Docket

- The Millennial Generation's Wireless Work Styles: Cutting Edge or Slippery Slope? (April 2009). The newest generation of tech-savvy workers, nicknamed the "Millennial" generation, face unprecedented exposure to security breaches. What are the risks and what strategies should in-house counsel wage to protect sensitive company information? www.acc.com/docket
- Debunking the Work-Life Balance Myth: Is it Fact or Fiction? (July/Aug. 2007). While a corporate legal department may not be the ideal environment to foster a balance between work and life, is it even possible to achieve? Here, the authors look at the obstacles standing in the way of in-house counsel attempting to strike that balance in order to find out if work/life balance is in fact possible or if it is merely a myth. www.acc.com/docket
- Small Law: Live to Work or Work to Live? (July/Aug. 2007). Read Todd Silberman's insights on the balance between work and life. Do we live to work or work to live? www.acc.com/docket

#### **Program Materials**

- We've Got An Eye On You: Employee Monitoring and Communications, Privacy, and Data Security (Oct. 2008). This program looked at the laws governing employee and customer monitoring and suggested best practices in connection with company policies and practices.
- www.acc.com/legalresources/resource.cfm?show=163818
- The Latest Technology for Law Department Management (Dec. 2007). Does your department have technology envy? Let our in-house experts help you find more time in your day by updating you on the latest software and other

technology available to help you manage claims, corporate filings and project development — all to assist you with running your legal department more efficiently. www.acc.com/legalresources/resource.cfm?show=19932

#### **ACC Alliance**

Looking for trusted service providers that provide high quality legal solutions? Look no more. The ACC Alliance partners offer exclusive savings on the services you need. Review the partners and their unique in-house counsel offerings at *www.acc.com/alliance.* 

#### **Sample Forms & Policies**

- Model Association Telecommuting Policy (Feb. 2009). This sample telecommuting policy includes supplemental guidelines of implementation, a telecommuting summary, and a compressed work week questionnaire. www.acc.com/legalresources/forms
- Remote Teleworking Program Policy Flexible Work Option, Fannie Mae (Jan 2007). Teleworking enables employees to work from home, in an alternative office space, or through a mobile office setting. Teleworking also adds flexibility to the workday. Read Fannie Mae's policy and see if their recommendations work for you and your company. www.acc.com/legalresources/forms
- Work at Home Policy (Oct. 2006). This document is a sample policy for a company offering alternative work arrangements. www.acc.com/legalresources/forms

ACC has more material on this subject on our website. Visit *www.acc.com*, where you can browse our resources by practice area or use our search to find documents by keyword. The only current federal regulation is of the disclosure of location records. A federal statute, 18 U.S.C. § 2702, prohibits electronic communications providers from disclosure of communication records, including the customer's location data.

There are few state statutes prohibiting the use of GPS to track employees. RFID legislation has been signed into law in New Hampshire, Utah, Virginia, Wisconsin and Wyoming.<sup>14</sup> A Wisconsin law (Wis. Assem. 290) prohibits any person from requiring another individual to have a microchip implanted in his or her body.

#### Tort of "Intrusion into Seclusion"

To establish intrusion into seclusion, an act must be "highly offensive."<sup>15</sup> For several reasons, the courts have been uninterested in expanding this tort to cover tracking devices. Primarily, the courts have found that if an employee uses company property like a cell-phone or GPS equipped vehicle, the employee is waiving rights to privacy.

#### Employer's Duty to Inform Employees

Employers certainly should want to inform most employees of tracking devices, because this undercuts any argument that the employee had a reasonable expectation of privacy. But does the employer have a legal obligation to advise employees? Cases like the 1996 *Smyth v. The Pillsbury Co.* case suggests that the employer does not, at least when the tracking is limited to work activities and premises. Whether an employer is required to inform employees when the tracking goes into off-work time or off premises, is beyond the scope of this article.<sup>16</sup>

Several states have statutes requiring notice of electronic monitoring, including Connecticut (C.G.S.A. §§ 31-48d, 31-511bb) and Delaware (19 Del. C. § 705).

#### **Issues in a Unionized Environment**

Introduction of a GPS device can raise diverse issues, particularly in a unionized environment. Where there is a collective bargaining agreement that gives a company the authority to update technology, it is appropriate for the employer to require its employees to use GPS devices. <sup>17</sup>

When GPS technology was introduced to unionized elevator constructors, for example, this raised issues over the employer's ability to track the employees "every move." The company, on the other hand, wanted to use the GPS tracking as a time clock on overtime call-backs, and only agreed to compensate the employees for time worked as shown by the GPS device.

When the employees complained, the company instructed the employees to turn the GPS devices off when they were not contractually required to have them turned on. But the company disciplined four employees who disabled the device on a weekend, even though they were on call. The dispute over tracking escalated — resulting in a work stoppage — and the company sued to enjoin it.

The court noted that all of the issues between the company and the employees emanated from their concern about the GPS monitoring. Because GPS is new technology and "similar disputes are likely to arise as the parties work towards a mutually agreeable call-back system," the Court granted an extensive injunction prohibiting strikes over disputes regarding overtime work assignments and the use of GPS technology as in the 2006 case *Kone, Inc. v. Local 4*, (International Union of Elevator Constructors).

#### **Discipline Based on Employee Monitoring**

Some companies have agreements with employees not to discipline or terminate them based solely on GPS tracking.<sup>18</sup> In that case, employees sometimes complain that any connection to GPS data invalidates the discipline.<sup>19</sup>

#### Discriminatory Use of Employee Monitoring Devices Based on a Protected Category

Employees have objected to the use of GPS, claiming that it has been used in a discriminatory manner

## **Monitoring and Surveillance Policy**

All computer, electronic and telephone documents, information and communications transmitted by, received from, or stored in any of the company's equipment is the property of the company. Employees are not to use any of the company's equipment, including office equipment, computers, software, facsimile, copy machines, telephones, vehicles or other equipment for their personal needs.

The company may track the employee's usage of its property, including but not limited to use of its computers, telephones, electronic equipment, vehicles and its other property. By using any of the equipment, employees consent to monitoring and review of the information obtained through monitoring by the company.

The use of a password does not give rise to an expectation of privacy. Employees must provide copies of passwords to the employer so the employer may have access at all times. Deleted messages and information may be maintained on the system and will be accessible for review.

Employees may be disciplined for any violation of company policy detected by monitoring. to monitor activities. Where, though, other employees also had monitors in their vehicles and all vehicles were on a plan to have GPS installed, an employee's belief of discrimination is not objectively reasonable.<sup>20</sup> In one case, for example, a GPS tracking was placed in the Plaintiff's vehicle to conduct an investigation, but similar tracking devices was also placed in company vehicles assigned to Caucasian employees, therefore, installation of the monitoring device was not racially motivated.<sup>21</sup> Moreover, an investigation using GPS that does not result in any discipline or employment loss does not constitute any adverse employment action against the employee.

#### **Statutory Proscriptions Do Not Prohibit Use of GPS**

Some states, such as Virginia, have statutes that restrict an employer's ability to electronically monitor employees in areas designed for health or personal comfort. However, it has been held that an employer's use of GPS to monitor a vehicle does not constitute electronic monitoring on premises and therefore the statute does not prohibit tracking through the use of GPS.<sup>22</sup>

#### Model Policies

A Model Policy on Electronic Monitoring is published by the National Workrights Institute on its website at *www. workrights.org/issue\_electornic/em\_model\_policy.html.* 

#### Implement Tracking Technology with Policies

The use of technology to track employees is becoming a common issue in the workplace and it has its proponents and its detractors. The jury is still out on whether enhanced productivity will outweigh privacy concerns. It remains to be seen whether employers or employees will embrace tracking systems.

But technology offers assistance in assuring that an employee is where he or she should be, and helps to keep employees productive. Employers concerned about employees' reactions to privacy issues, can enact policies that balance the employer's needs with the employees' interests. Employers should be cautioned against throwing out the baby with the bathwater, since there are many potential benefits to harnessing technology to assist in monitoring an employee's productivity and since the courts have generally supported employers' efforts to do so.

Have a comment on this article? Email editorinchief@acc.com.

#### NOTES

- 1 Schachte and Swanson, *Workplace Privacy and Monitoring, New Developments Affecting the Rights of Employers and Employees,* Practicing Law Institute, PLI Order No. 8966 at p. 10.
- 2 Finch v. Schneider Specialized Carriers, Inc., 690 N.W.2d 699

(Iowa 2004), vacated other grounds 700 N.W. 2d 328 (Iowa Sup. Ct. 2005).

- 3 R. Gellman, "A General Survey of Video Surveillance Law in the United States," in: J. Nouwt, B.R. de Vries and J.E.J. Workplace Privacy, IT & Law Series 7, Den Haag: T.C.M. Asser Press (2005).
- 4 See, e.g., *Brannen v. Bd. Of Educ.*, #CA2000-11-098, 144 Ohio App. 3d 620, 17 IER Cases (BNA) 1405 (Ct. App. 2001).
- 5 See, e.g. The Dartmouth.com news April 27, 2007, reported at *http://thedartmouth.com/2007/04/10/news/experts/.*
- 6 Balkovich Bikson and Bitko, "9 to 5: Do you Know if Your Boss Knows Where You are? Case Studies of Radio Frequency Identification Usage in the Workplace" (2005).
- 7 Morrissey, "Are Microchip Tags Safe?" *Time*, October 18, 2007, *www.verichipcorp.com/news/1192716360*.
- 8 These Last Days Ministries, Inc. 1996 2006, www.tldm.org.
- 9 See Dennis R. Nolan, Privacy and Profitability in the Technological Workplace, 24 J. Lab Research 207, 209-210 (2003) In relation to issues such as employee blogging, the courts have also held that private employees do not have a right to protect them from being terminated because of the exercise of constitutional free speech. *Edmondson v. Shearer Lumber Products*, 75 P. 3d 733 (Idaho 2003).
- Marrs v. Marriott Corp, 830 F. Supp. 274, 283 (D. Md. 1992) (No reasonable expectation of privacy in an open office, where an employee was videotaped picking a lock on a desk drawer).
- 11 "While the issue has not been decided under the Fourth Amendment, the New York Court of Appeals has held that unless there is an exception to the warrant requirement, warrantless placement of a GPS device on the exterior of a vehicle violates the New York State Constitution. *People v. Weaver*, 12 N.Y.3d 433 (2009).
- 12 *Kyllo v. United States*, 533 U.S. 27, 34 (2001)(using heat-sensing technology).
- 13 Location Privacy Protection Act of 2001, Senate 1164 (107<sup>th</sup> Cong. 1<sup>st</sup> Session [1999].
- See, Assem. 290, 97<sup>th</sup> Leg. Reg. Sess (Wis. 2006); H.R. 204, 159th Gen. Ct., Reg. Sess. (N.H. 2005); H.R. 185, 2005 Leg. Reg. Sess. (Utah 2005); H.R. 258, 58th Leg. Reg. Sess. (Wyo. 2005); S. 148, 2004 Gen. Assem., Reg. Sess. (Va. 2004).
- 15 Miller v. Nat'l Broadcasting Co., 187 Cal. App. 3d 1463 (Cal. App. 2nd Dist. 1986). Monitoring generally does not qualify because it does not involve a physical intrusion. Dan Long, the Electronic Workplace, Modrall, Sperling, Roehl, Harris & Sisk, P.A., June 3, 2002; but see Ruzicka Elec. And Sons, Inc. v. International Broth. Of Elec. Workers, 427 F.3d 511 (8<sup>th</sup> Cir. 2005).
- 16 The Oregon Supreme Court's opinion in *State v. Meredith*, 337 Ore. 299, 96 P.3d 342 (2004) suggests that the rules might be different for non-employment tracking, since the court found it critical that the employee did not have a privacy interest in keeping work-related locations and activities private.
- 17 Otis Elevator Co., v. Local 1, 2005 WL 2385849 (S.D. N.Y. 2005).
- 18 See, e.g., Smith v. Pacific Bell Telephone Co., 2007 WL 1114044 (E.D. Cal. 2007).
- Hinkley v. Roadway Express, Inc., 2006 WL 2522522 (D. Kan. 2006), aff'd, 249 Fed. Appx. 13 (D. Kan. 2007).
- 20 Brantley v. Muscogee Cty. School Dist., 2008 WL 794778 (M.D. Ga. 2008).
- 21 Elgin v. St. Louis Coca-Cola Bottling Co., supra, note 19, 2005 WL 3050633 (E.D. Mo. 2005).
- 22 Vitka v. City of Bridgeport, 2007 WL 480 1298 (Ct. Super. 2007).

# OUTPERFORM EXPECTATIONS®

- Recognized as a Go-To Law Firm<sup>®</sup> for corporate transactions, labor and employment, intellectual property, international, litigation and securities by Fortune 500 general counsel (*Corporate Counsel*, 2009)
- Ranked among the top 20 law firms in the United States for client service (BTI Consulting Group, 2009)

More than 500 lawyers in the United States, England and China.



MORE TOGETHER www.faegre.com