Monitoring Employees in the Modern Workplace: Can a GPS Result in TMI?

Publication
2.13.14

The answer is "yes" – tracking employees by using Global Positioning Systems can give an employer Too Much Information.

Background - Surreptitious Surveillance

In 2012, the United States Supreme Court held (in the case of U.S. v. Jones) that the government's attachment of a Global Positioning System (GPS) to the vehicle of an individual suspected of drug trafficking was a "search" within the meaning of the Fourth Amendment (which provides protection against unreasonable searches) and thus required a warrant.

Following the Jones decision, a New York court found last year that a public employer (ironically, the New York Department of Labor) who attached a GPS to the car of an employee (*Cunningham*) had engaged in a search; however, the New York court was of the opinion that the Supreme Court had left open the question of when, if ever, a GPS search was permissible without a warrant.

In the *Cunningham case*, the New York Department of Labor attached a GPS to the employee's car, without the employee's knowledge, because it suspected the employee of submitting false time reports; naturally, the GPS seemed an effective way to accurately determine whether the employee was at his office during the times he claimed or, as suspected, having an out-of-office rendezvous with his secretary.

The New York court determined that a warrant was not required, finding that the parameters of the search fell within the "workplace exception" previously sanctioned by the Supreme Court. This workplace exception permits warrantless searches by public employers in work areas where an employee would have no reasonable expectation of privacy. Nevertheless, the New York court found that the Department of Labor's use of the GPS in this case was unreasonable because it tracked activity during times in which the Department had no legitimate interest, i.e., evenings, weekends, and vacations (with the secretary).

One of the judges in the *Cunningham case* filed a separate opinion and criticized the other judges' finding that the installation of the GPS system was permissible without a warrant. This judge explained that, regardless of the workplace exception, there could be private information, outside of

workplace, that inevitably would be disclosed in the data retrieved from a GPS placed on an employee's personal vehicle – for example: "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." On some matters, ignorance is bliss.

The Private Sector

While the Fourth Amendment does not apply to private employers, some states have enacted laws making it illegal for a private employer to place a location tracking device on an employee's vehicle without the employee's consent. Interestingly, a few states have even adopted legislation prohibiting employers from implanting GPS-like microchips in the form of Radio-frequency identification (RFID) under an employee's skin.

Tennessee

In Tennessee, it is a misdemeanor for anyone other than a car manufacturer, a law enforcement officer in pursuit of a criminal investigation, or a parent of a minor to "knowingly install, conceal or otherwise place an electronic tracking device in or on a motor vehicle without the consent of all owners of the vehicle for the purpose of monitoring or following an occupant or occupants of the vehicle." Tennessee Code 39-13-606.

Employer-owned Equipment

Employers have various reasons for wanting to monitor employee whereabouts, ranging from safety concerns to ensuring compliance with company policies and procedures. There can be legitimate uses of tracking devices placed in company-owned vehicles. For example, in the shipping and logistics industry, tracking a vehicle's location may be useful to estimate and confirm delivery times. Some trucking companies monitor the driving hours of employees to ensure compliance with Department of Transportation regulations requiring drivers to take breaks after driving a certain number of hours. A driver who exceeds the permissible number of driving hours and falsely reports his sleeping vs. driving time could be found guilty of misconduct when faced with evidence derived from a GPS log contradicting his reports.

Employees have concerns, however, that private information derived from monitoring systems might influence employers when they are making decisions about work assignments or promotions. Beyond privacy interests, employees also are apprehensive about the accuracy of information employers might derive from these systems. There are concerns that GPS monitoring might make it appear that an employee is engaging in inappropriate activity when that is not the case. For example, an employee who has to take a detour because of road work might be accused of taking an impermissible side trip; or, sitting in a traffic jam could look like idling or an impermissible stop.

What about smartphones? It follows that tracking a smartphone can be even more intrusive than tracking a car because the employee likely will take the smartphone into those private places envisioned by the Cunningham judge and listed above.

How Much is Too Much?

Employers should be wary of monitoring employees without their consent for any reason. A carefully drafted Employee Handbook can serve an employer well by clearly explaining that the employee should have no expectation of privacy in company-owned equipment. Any kind of monitoring should be closely tailored to suit a particular employer's legitimate business needs and should be limited to working hours. Monitoring employees outside of these parameters will run the risk of being deemed an unreasonable invasion of employee privacy and could lead to claims of discriminatory treatment based on information inadvertently obtained and relating to private matters. In some circumstances, more knowledge is not always a good thing.

This article appeared in the February 2014 issue of *HR Professionals of Greater Memphis.*

Service Focus

Privacy and Cyber