
ORANGE COUNTY
Attorney
JOURNAL
Volume 114, 2015 • $6.95
Outsource Your Marketing, Not Your Life
Stephen Fairley
Incorporating Creative Landing Pages to Get Clients
Landon Biehl
McIntyre's Civil Alert Organized Succinct Summaries
Monty A. McIntyre
Mergers Have Increased Substantially this Year, but Pay Attention to the Red Flags
Robert Denney
Big Brother, Big Liability
Todd Wulffson and Emily Borman
How to Handle Negative Facebook Reviews
Travis Haney
Keeping Top Legal Performers on for the Long Haul
Whitney Price
Attorney of the Month
Co-Founder of Brown & Charbonneau, LLP
Gregory Brown
The Go-To Trial Lawyers for Business & Complex Family Law Litigation

BIG BROTHER, BIG LIABILITY

by Todd Wulffson and Emily Borman

With today's advanced technology, how much employee monitoring is too much?

Like the Orwellian "Big Brother" looming omniscient from the pages of 1984, employers today possess the ability to track virtually every aspect of their employees' lives—including off-duty activities. Video cameras, email and computer monitoring, Global Positioning System (GPS) tracking of smartphones and cars and even drones, are all tools the modern employer has at its disposal. Workplace privacy is rapidly becoming a thing of the past, and many employees do not even know how exposed they are.

Of course, technology has also given employers increasingly good reasons to monitor their employees. With the advent of the internet and its progeny—instant messaging, smartphones, social networking, online pornography and gambling—and the rise in internet-dependent telecommuting, the potential for workplace distractions and the risk of employer liability for employee misconduct is at an all-time high.

The question for employers is how much monitoring is necessary, appropriate and legal. After all, no employer wants to suffer the added insult to injury of firing an individual for misconduct, only to lose an invasion of privacy lawsuit filed by the same former employee.

PRIVACY RIGHTS OF EMPLOYEES

Article 1, Section 1 of the California State Constitution explicitly protects a person's right to privacy and applies to both public and private employment settings. When an employee sues an employer for unlawful monitoring, it usually goes to court as a generic invasion of privacy claim. To bring an invasion of privacy claim, the employee must establish a reasonable expectation of privacy under the circumstances.

Courts have been reluctant to determine a reasonable expectation of privacy exists where employees are aware that the employer may intrude upon their privacy for legitimate business purposes. For example, when the employer properly notifies the employee in advance that email and computer activity may be monitored, and that employees' desks, lockers, backpacks and purses may be searched, courts have generally ruled that no invasion of privacy has occurred. Where the employer's monitoring goes beyond legitimate business purposes, however, and intrudes on what society may be considered highly personal areas, an actionable invasion of privacy may be found, with emotional distress and punitive damages as a result.

USE OF COMPANY LAPTOPS AND SMARTPHONES

In the modern office, internet access and e-mail have become ubiquitous, and many employees use wireless communications such as a smartphone and laptop in the day-to-day performance of their jobs. Often these devices are provided by the company or supported (financially and technically) by a "Bring Your Own Device" (BYOD) policy. The need to secure

confidential information, monitor customer communications and investigate potential employee misconduct has led to an increase in the monitoring of these devices, commensurate with their increased usefulness.

California courts have been reluctant to find that employees have a reasonable expectation of privacy in their personal use of an employer-provided computer or smartphone. This is especially true where the employee has notice of company policies that preclude employee rights of privacy in their use of company equipment.

In a recent California case on the subject, an employee contacted her personal attorney on a company-issued computer using her company email account. The court found the emails were not protected by either a right of privacy or the attorney-client privilege. Using the company account and system waived the privilege, and company policies precluded any expectation of privacy. The employer had issued policies that company machines could only be used for business purposes, and that any communications might be monitored.

GPS TRACKING

The use of GPS tracking devices to monitor employees during work hours has also been deemed by California courts to be reasonable. GPS technology, however, enables employers to monitor employees 24 hours per day, seven days per week. If the employer is tracking its employees outside of work hours, the employer may gain private information about an employee that would be considered an invasion of privacy. It is this type of off-duty monitoring that generates the most litigation.

In a recent case in California, an employee of a financial services company told his boss that he was sick and would have to miss a critical meeting with clients that day. Later that same day, at 2:00 p.m., the employer tracked the employee's smartphone and found that he was lounging poolside at a Las Vegas casino, more than 250 miles away from his home in California.

When the employee came back to work, the employer asked why his phone was in Vegas while he was sick at home. The employee said he got better, so he left for the trip. The employer fired him. The lawsuit eventually settled for no money, aside from the legal fees incurred by the employer in defending the frivolous lawsuit. Had the employer used that technology over the weekend, however, the result might have been far different, as the employee had not been notified that there was GPS tracking on his phone and would have had a reasonable expectation of privacy.

Employers also use GPS to track the location of company cars. As with the company phone, employers should limit such monitoring to what is necessary to protect the employer's interest, i.e., only during working hours and/or total mileage. Employers should also notify employees that company cars are monitored, which in and of itself may deter the misuse of the company vehicle.

RISE OF THE DRONES

Although the rise of drones has opened the door to countless possibilities related to monitoring and oversight, the business community has only begun to explore their capabilities. Before adding drone surveillance as an employee monitoring tool, there are several pitfalls an employer should be mindful of, including the perception that drone use is scary and futuristic.

In one case, an employer managed a construction site in California, where employees worked largely without supervision. The structure they were building was still a skeleton, with employees installing electrical wires on the top floors before the walls went up. The employer sent a drone up to the fourth floor of the building to monitor the workers, and two employees were having sex during an alleged mutual break. Both employees were fired and sued, arguing that no one on the ground level could see them on the fourth floor, and the company wouldn't have known of their activities had it not been for the drone.

This case settled in the employees' favor, primarily due to the negative publicity the company would have encountered had their surreptitious drone use become public. Even if the employer had advised its employees of the drones (assuming the employees did not all quit thereafter), a jury might still have found the use of the drone to be unreasonable, similar to night vision, a high magnification lens on a camera or a parabolic microphone.

BEST PRACTICES

While there are no guarantees that any monitoring of employees will prevent your company from being sued, the following best practices will help minimize potential liability:

1. **Assess the need for any monitoring.** What conduct are you trying to prevent? Consider hiring a third-party specialist to assess the need for monitoring.
2. **Do a cost-benefit analysis.** What will the true cost of monitoring be, including the potential lawsuits and risk to morale, and compare that to the benefit of deterring—not eradicating—the misconduct.
3. **Have a clear, concise policy that states the need for monitoring, necessary details, and the consequences for getting caught.** A good policy will go a long way toward deterring the conduct, and will avoid a majority of the liability risk (although perhaps not the damage to morale caused by Big Brother monitoring employees).

4. **Make sure a legitimate business interest exists for monitoring.** For every level of monitoring or intrusion, there must be a reason consistent with company policy.
5. **Ensure that all monitoring, as well as all discipline arising from the monitoring, is performed by trained individuals.** They should know and understand the law, and apply your company policy consistently across all similarly situated employees.

Technology is key to business in today's world, but remember to keep your employees' privacy rights in mind when using it as an oversight tool; no employer should channel Big Brother in the workplace. ■

Todd R. Wulffson is partner at Carothers DiSante & Freudenberger LLP, a leading California employment, labor and business immigration law firm providing litigation defense and counseling to California employers. Wulffson has 25 years of experience counseling and defending businesses in labor and employment issues and has extensive experience representing employers across the entertainment, manufacturing, banking, hospitality, financial services and retail industries. Wulffson focuses on issues related to human resources, and the implementation of proactive measures to reduce risk and cost including substantial experience in the evolving area of Social Media Law. He is a frequent speaker, author and resource to employers nationwide on analyzing employee-related social media issues, preparing social media policies and procedures, and defending actions involving social media liability claims. To contact Wulffson, email him at twulffson@cdflaborlaw.com or call (949) 622-1661.

Emily K. Borman is an associate attorney at Carothers DiSante & Freudenberger LLP, a leading California employment, labor and business immigration law firm providing litigation defense and counseling to California employers. Borman defends employers against allegations of wrongful termination, harassment, discrimination and retaliation. In addition, she also defends against wage and hour claims whether brought as a putative class action, or on behalf of an individual plaintiff. Borman's practice strengths include navigating through the difficult procedural hurdles present in class action litigation. To contact Borman, email her at eborman@cdflaborlaw.com or call (949) 622-1661.