Monitoring Employee Conduct Outside of the Workplace

Karl W. Butterer, Esq. and Laurence D. Lieb, CCPA
Foster Swift Employment, Labor & Benefits News
November 17, 2016

AUTHORS/ CONTRIBUTORS
Karl W. Butterer

PRACTICE AREAS
Employer Services
Employment Law

In the not too distant past, employers and employees had a clearer idea of what was, and was not, part of the workplace. In the past two decades, both employers and employees have blurred that distinction through changing technologies and work habits. At the same time, technological leaps have made it increasingly cheap and easy for employers to electronically monitor employee conduct. Employers must consider both the benefits and risks of electronic monitoring, and respect the legal limits on such monitoring.

THE INCREASINGLY BLURRY LINE BETWEEN WORK AND HOME

It is not so easy anymore to tell if an employee is engaged in work or personal business at any given moment. Employees now access employer computer networks from home both during and outside of regular working hours. Employees regularly connect with one another by email at all hours and from virtually any location. Employees often use employer owned computers both in and outside of the traditional workplace to engage in social media, shopping and personal business. Employees are increasingly bringing their private electronic devices to work to conduct private business, as well as to connect to company networks. With greater frequency, employees are installing privately registered applications, like Messenger, Facebook or What's App, on employer devices to communicate outside of the employer's networks.

NEW TECHNOLOGIES FOR MONITORING EMPLOYEE CONDUCT

Employers now have a number of increasingly powerful tools to electronically monitor employee conduct on workstations (laptop or desktop computers), smartphones, and email servers. For smartphones, employers may now install **Mobile Device Management** software onto both company-owned and employee-owned smartphones, which allows the employer to monitor and record the following categories of information:

- Internet browsing activity
- Real time physical locations of smartphones

- Social Media activity performed on smartphones
- Passwords entered on the smartphones
- Email and text message communication sent and received by smartphones
- Photographs and videos created and received by smartphones
- Files being created on, sent and received by smartphones

For workstations, employers can install software that monitors and records the following categories of information in real time:

- Screen captures
- File and document related activities such as copying and printing
- Email usage
- Access of company file servers
- Web browsing activity
- Instant message activity
- Application usage
- Keystroke captures

Employers can set up alerts to flag specific activities such as accessing of inappropriate websites by employees.

Employers can monitor real time activities on company email server systems, such as the recipient email addresses an employee is using. For example, to protect customer data, financial sector companies oftentimes set up alerts to notify the employer when an employee sends an email to a Gmail or Yahoo email account address.

WHY MONITOR?

Employers have legitimate motives to electronically monitor employee conduct, such as to:

- Prevent the unlawful transfer of employer trade secrets and protected intellectual property.
- Investigate and prevent the unlawful discriminatory harassment of fellow employees.
- Stop or limit non-work related internet activity during work time and/or while using employer devices to shop, engage in social media, visit inappropriate websites, use excessive bandwidth, or conduct personal business.
- Capture electronic communications or records which may be the subject of "litigation holds" or corporate record keeping policies.
- Stop the dissemination of customer or patient information, such as confidential financial records or protected health information under HIPAA.

LEGAL LIMITS ON MONITORING

There is no single law which sets out the limits on employer monitoring. Below are a few of the more significant laws of which employers should be aware before undertaking monitoring.

The **Fourth Amendment** to the United States Constitution prohibits a government employer from engaging in the unreasonable search of things in which an employee has a reasonable expectation of privacy. Whether an employee had a reasonable expectation of privacy in information on a computer or smartphone often turns on whether the government employer made a clear disclosure that the employee's use of the technology would be monitored. In some cases, the government employer's motive for the search will impact whether the search is lawful. For example, in *City of Ontario v Quon*, a court found that the search of an employee's text messages did not violate the Fourth Amendment because the employer was trying to determine whether the employee's excessive texting was work-related or for personal use.

Both public and private employers should review any applicable **collective bargaining agreement** (CBA) to ensure that the contract does not prohibit monitoring. Even if the CBA does not prohibit the monitoring, the employer should consider whether the decision to monitor can be made unilaterally by the employer, or it is a change in working conditions that must be negotiated with the union. Similarly, both private and public employers must be familiar with **Michigan's common law**, which prohibits an employer from using an unreasonable means or method to intrude upon a matter in which an employee has a right of privacy.

Several federal and state statutes impact if, and under what circumstances, an employer may gain access to electronically stored information. The **Stored Wire and Electronic Communications and Transaction Records Act** (SECA) creates a private cause of action, as well as potential criminal penalties, for the intentional and unauthorized access to "a facility through which an electronic communication service is provided." The **Internet Privacy Protection Act** (IPPA) prohibits employers from asking employees to grant access to or allow observation of employee internet accounts. Significantly, IPPA contains important exceptions for employers, such as where the employer pays for the device, provides the account or service, or is conducting certain kinds of investigations. Michigan's **Bullard-Plawecki Employee Right to Know Act** generally prohibits an employer from gathering or keeping a record of an employee's associations, political activities, publications, or communications of nonemployment activities. However, an employee may authorize such monitoring in writing. The prohibition also does not apply to activities that occur on the employer's premises or during working hours which interfere with the performance of the employee's duties or that of other employees.

CONCLUSION

Employers have legitimate reasons, and increasingly effective tools, to lawfully monitor employee conduct which takes place outside of the traditional four walls of the workplace. In making monitoring decisions, employers must respect employees' constitutional, common law, statutory, and sometimes contractual rights to limit monitoring. Of course, with monitoring as with anything else, just because you can do it, does not mean you should do it. The authors can help you weigh the costs, benefits and risks of a monitoring decision.