Protecting Trade Secrets Through Employee Surveillance: Risky Business

Insights
3.14.11

The difference between having a trade secret and not can come down to the steps that a company takes to protect its secrets. The Uniform Trade Secrets Act, a version of which has been adopted in 46 states, provides that information qualifies for trade secret protection only if the owner takes steps that are reasonable under the circumstances to protect its secrecy. Employers commonly take the obvious steps to protect their trade secrets – for example, requiring employees to sign confidentiality agreements or restrictive covenants, implementing electronic controls; and let's not forget sending demand letters and threatening litigation. These steps are obvious and therefore widely observed. But what about proactive monitoring? If you have a trade secret, you ought to keep an eye and ear out to make sure it's not being used or disclosed. But, be careful; doing so is not without its risks.

With recent (and not so recent) advances in technology, employers have substantial means at their disposal to monitor their employees' conduct and communications.Available options range from reviewing employees' email communications and computer usage to monitoring telephone discussions.In general, these tactics are lawful unless specifically prohibited by statute or the employee has a reasonable expectation of privacy under the circumstances.

Surveillance of Employee Email

The Electronic Communications Privacy Act, 18 U.S.C. § 2510 ("ECPA") was originally enacted to address the interception of wire, oral and electronic communications.The statute was specifically amended to cover email communications. Under the ECPA, electronic communications may be intercepted with the consent of one party to the communication, or under certain conditions, by a service provider if necessary incident to the provision of the service or to protect the provider's rights and property.Some courts have held that a "service provider" includes an employer who provides email access to its employees.The "service provider" exception becomes even stronger if the employer is monitoring emails once they are in storage (as opposed to during transmission) because such communications are subject to Title II of the ECPA, known as the Stored Communications Act ("SCA").

Despite these employer friendly exceptions under the ECPA/SCA, employers can make life easier for themselves by obtaining the express written acknowledgment and consent of employees.To this end, employers should provide employees with clear and simply written policies noting the employer's right to monitor all employee communications that involve the use of employer-provided technology.It is a good idea to require employees to sign a written statement that they have been advised of the employer's right to monitor communications.Employers might even consider providing employees with electronic notification of these rights that requires employees to manually acknowledge receipt of the employer's policy and understanding of its content through the clicking of certain boxes on screen.Posting open and conspicuous notices throughout the work area will likewise serve to establish that employees lacked a reasonable expectation of privacy in their electronic communications. (While you are at it, a well written policy may make the difference between having and not having a claim under the Computer Fraud & Abuse Act.)

Monitoring Use of Computers

Employers often provide employees with computers to use for work purposes that are capable of accessing workplace computer networks via direct and/or remote internet access.Employees commonly can access the internet from workplace computers enabling them to receive and transmit information related to the employer's business.Employers should reserve, and just as importantly, employers should exercise, the right to monitor employees' activities on these networks and via the internet.The need to do so is heightened when there is cause to believe an employee has engaged in misconduct.As with email communications, it is prudent to unambiguously advise employees that their activities are subject to monitoring, and to require their express acknowledgment.

Surveillance of Telephone Communications

Interception of telephone communications is yet another way to monitor the use and potential misuse of your trade secrets, but it is here that the ECPA has great potential to apply.The ECPA generally prohibits interception of telephone calls, but a number of notable exceptions leave employers well positioned to monitor such calls.The most notable includes interception with prior consent.Consequently, if an employer intends to monitor telephone calls, the strongest form of consent is express consent.Consequently, the best practice requires that employees should be

informed and their consent obtained in writing.This will leave little room to doubt whether employees had a reasonable expectation of privacy in their communications.As noted below, some state laws require consent of all parties to the communication.For this reason, we have all heard at one time or another the prerecorded message that "this call may be recorded for quality assurance purposes."In the absence of express written consent, other exceptions may apply.Consult your counsel for details.

A Final Thought

As noted at the beginning of this article, employers are generally free to monitor their employees unless specifically prohibited by statute.Federal statutes such as the National Labor Relations Act (NLRA) and the Labor Management Relations Act (LMRA) impose significant restrictions on employers' abilities to monitor the union organizing activities of employees.In addition, the ECPA does not preempt more stringent state laws, and accordingly, many states offer greater protection.For example, California, Delaware, Florida, Massachusetts, and Pennsylvania are a handful of the many states that require "two-party consent" before an employer can intercept or record a telephone call in real time.Similarly, Delaware and Connecticut have enacted statutes that address email monitoring.Consequently, employers operating in multiple states or communicating with third parties from other states are wise to consider state law.

The bottom line?If you have a trade secret, proactive monitoring of employees to protect your trade secret rights is worthwhile, but not without risks.Consult your counsel and come up with a plan that balances your need to police use and disclosure of your trade secret, on the one hand, with the statutory rights and reasonable privacy expectations of your employees, on the other hand.

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either follow Michael R. Greco on Twitter or on LinkedIn or subscribe to this blog's RSS feed.

Related People

Michael R. Greco

Michael R. Greco
Regional Managing Partner
303.218.3655
Email