The Legal Intelligencer

An Employer's Duty to Report Crimes by Employees to Police

Over the past decade, many European countries have passed laws mandating that individuals and employers report criminal conduct.

Hayes Hunt and Jonathan R. Cavalier

2012-04-18 12:00:00 AM

Over the past decade, many European countries have passed laws mandating that individuals and employers report criminal conduct. In the United States, however, individuals are typically not required to report criminal conduct that they have observed.

Likewise, employers have no general duty to report criminal conduct by their employees. Often, this lack of an affirmative duty or any other incentive to report criminal conduct will lead an employer to simply look the other way, rather than risk disrupting workflow, losing a valuable employee, bringing negative publicity on the company or facing liability for invasion of privacy or defamation.

However, not all situations are created equal, not all crimes are treated the same and exceptions exist that may require employers to report the criminal actions of their employees. Consider the following hypothetical scenarios:

• Scenario 1: An employee uses his personally owned iPad for work purposes. He uses the iPad for work when he travels and takes work home with him on it. The employee brings his iPad in to have the employer's IT personnel fix a problem with his email accounts. While performing maintenance, the IT department discovers child pornography on the device. Should the employer report the employee to the authorities? Must the company report the employee and, if so, to whom?

This is perhaps one of the more difficult situations that an employer can face. Unfortunately, with the proliferation of technology and the intermingling of employer- and employee-owned technology, this situation arises more frequently than anyone would care to admit. When it does, the employer is often confronted with a problem of balancing the need (and desire) to report such an employee to the authorities with the potential exposure resulting from the employee's potential privacy rights.

Recent changes to federal law have made the answer to this problem clear: The employer must report the employee. 18 U.S.C. §2258A requires any provider of an "electronic communications service" or "remote computing service" to report information about the employee, including identity, email and IP address, or any other identifying information, to the National Center for Missing and Exploited Children. An "electronic

communications service" is defined by the law to include "any service which provides to users the ability to send or receive wire or electronic communications." In other words, any business that provides its employees with email is subject to the law, and penalties for violations are harsh. Many states have passed similar laws requiring similar reports.

In addition to these reporting requirements, at least one employer has been found liable in a civil lawsuit for failing to report child pornography found on a work computer. In the New Jersey case of *Doe v. XYC Corp.* , 887 A.2d 1156 (N.J. Super. 2005), an employee was, among other things, visiting child pornography sites while at work and sending photos of his 10-year-old stepdaughter to one of those websites, according to the opinion. He was later arrested for his conduct. The mother of the 10-year-old then sued XYC, alleging that the company knew, based on logs generated by the computer and complaints from other workers, that the employee was accessing child pornography at work. While he was reprimanded by the employer, his conduct was never investigated or reported. In reversing summary judgment in XYC's favor, the Appellate Division of the New Jersey Superior Court held that "an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third parties ... No privacy interest of the employee stands in the way of this duty on the part of the employer."

Given the gravity of the conduct involved, few employers will hesitate to report an employee found to be in possession of child pornography on employer-owed computing equipment. However, the situation can become muddied if the device in question belongs to the employee. For instance, an employee may use a personally owned smartphone or laptop for business purposes and may avail himself of the employer's IT department when in need of technical support. How can an employer ensure compliance with the law without exposure to liability for invasion of privacy?

The key to avoiding this conflict is to have clear policies on the use of electronic devices in the workplace. An employer should include in its company handbook clear language notifying the employee that (a) any employer-issued equipment remains the property of the employer; (b) the employee has no right of privacy in anything he or she does on that equipment; and (c) the employer may access and search the equipment at any time and without notice. Ideally, employees will be reminded of their lack of a privacy interest each time they log on to their computers.

However, with the proliferation of personal technology, many of these policies are limited to company-owned computers and, therefore, do not go far enough. These policies should be extended to cover employee-owned technology used by the employee on the job. In short, if an employee wishes to use his personal cellphone, laptop or tablet computer for work purposes, he or she may do so, but must waive any privacy right to the contents of the device and consent to searches of the device without future notice. At a minimum, employers should require consent to search and waiver of privacy for any devices used by the employee that are serviced by the employer's IT department. At most, employers may wish to ban use of employee-owned technology on the job entirely.

In addition to ensuring that the employer can comfortably comply with the reporting requirements described above, such policies are good business. They can help safeguard the employer's trade secrets and confidential information, as well as sensitive data that may belong to third parties or customers.

• Scenario 2: A Fortune 500 company is committed to developing a family-friendly workplace. The company has developed industry-leading flex initiatives, benefits for working mothers and extended pregnancy and child-care leave programs. The company has won numerous awards and is recognized as one of the best places to work for workers with children. One of the company's newest initiatives is an on-site, company-owned daycare center for children of employees. One daycare staffer notices that a 5-year-old child frequently arrives at the center with suspicious bruising on his arms and legs. What obligations does the employer have in such a situation?

All 50 states have passed laws regarding the reporting of suspected child abuse. While some states require anyone who reasonably suspects child abuse to report it, most states define certain specific groups of

professionals that must report such abuse. These groups typically include types of jobs that require regular interaction with children, like teachers, doctors, social workers and law enforcement officers. These laws generally require the reporter to call a designated reporting hotline and provide the suspected abuser's name and other identifying information. Some states allow the reporter to remain anonymous. In most states, a good-faith report of suspected child abuse provides immunity for the reporter.

In all states with such laws, daycare centers are designated as mandatory reporters of suspected child abuse, as are any people paid to care for a child in a public or private facility. Pennsylvania expressly mandates that any staff of a daycare center who has reason to believe that a child enrolled in the facility has been abused is required to report it. These laws cover and apply to daycare centers run as a benefit for company employees, even though the company is not in the "daycare business," and even though only company employees may take advantage of the program.

Employers that offer daycare services to their employees should take steps to train the employees staffing the daycare center about their reporting obligations and the steps that they must take to spot and report suspected abuse. Employees should be trained on the protections that the law offers for reports that are ultimately unfounded but made in good faith and explain that the employee will not be reprimanded for following policy, even if mistaken. The employer should also designate an HR person to field questions from daycare employees regarding reporting obligations.

Finally, employers should be aware that, depending on the state in which their business resides, mandatory reporting requirements for suspected child abuse may apply even if their business is not typically one associated with child care. Employers should know whether they are subject to mandatory reporting requirements in their state and advise their employees accordingly.

• Scenario 3: A salesperson for a manufacturing company is having a record-setting year. His sales are continually the best in the company. Another employee notices a competitor's price list and contacts sheet on his desk. When asked about these materials, the employee reveals that he used to work for the competitor and that, when he left, his former supervisor failed to disable his computer access. He has since continued to log in to his former employer's system to gain access to information that enables him to undercut his competition on price. What should his current employer do?

The employee above is likely breaking at least two federal laws. First, he is certainly violating the federal Computer Fraud and Abuse Act, which prohibits, among other things, knowingly accessing a protected computer with intent to defraud and to obtain anything of value. He is also likely violating Section 1832 of the Economic Espionage Act of 1996, which criminalizes misappropriation of a trade secret with the intent to convert the trade secret to the economic benefit of someone who is not the rightful owner. He is also likely violating a slew of state laws regarding computer fraud and trade secret protection.

It goes without saying that the employee should be severely disciplined for his conduct, which has subjected the employer to potential civil and criminal liability. The best course of action may be to terminate the employee. Should the employer report his conduct to the authorities? If the employer keeps the conduct of the employee in-house, the situation could blow over. This is a huge risk.

If, however, the conduct is discovered by the competitor, a lawsuit is sure to follow and the competitor may report the individual's actions to the appropriate authorities. In the latter situation, reporting the employee to the authorities would have gone a long way toward establishing that the employer does not authorize or condone such trade secret theft and that, when confronted with a rogue employee, the employer took swift and decisive action to prevent the conduct from reoccurring.

The key to avoiding this kind of dilemma is to prevent the criminal conduct from occurring in the workplace. Employers should institute a trade secret policy that clearly specifies that employees are not encouraged, authorized or permitted to use trade secrets or confidential information belonging to competitors and that, if an employee is caught using such information, he or she will be subject to severe discipline. By establishing and enforcing such a policy, employers can gain significant protection against suits for trade secret misappropriation and unfair competition. •

***Hayes Hunt**, a member of Cozen O'Connor in the firm's commercial litigation and criminal defense and government investigations practice groups, concentrates his practice in the representation of individuals, corporations and executives in a wide variety of federal and state criminal law and regulatory enforcement matters, as well as complex civil litigation. He can be reached at hhunt@cozen.com.*

***Jonathan R. Cavalier** is an associate in the firm's commercial litigation group. He has substantial trial experience, including experience as first-chair jury trial counsel. He can be reached at jcavalier@cozen.com*
