

## Headache #1: Porn on Work Computers

What can in-house counsel do when employees view, download, and forward abusive material?

BY ADAM P. PALMER  
AND SHERRI A. AFFRONTI

What are the risks for employers in instances where employees use company computers to access, view, download, store, and possibly forward pornography or engage in illegal activities? How can corporate counsel both prevent these abuses and handle investigations if they suspect some kind of prohibited conduct is occurring in the workplace?

Certainly, an employee's abuse of a company's computer systems can raise a number of legal concerns not only for the individual but

### Corporate Counsel

A Special Report

also for the corporation. For example, cases abound where the contents of employee e-mails, computer downloads, and other electronic communications are used as evidence in claims of discrimination or harassment in

the workplace. Central to such claims is proof that the employer failed to take appropriate steps to prevent—and promptly correct—the unwelcome conduct.

Aside from their concern over potential discrimination or harassment claims based upon the content of inappropriate e-mails and other electronic communications, companies have traditionally worried about a variety of tort claims which may be brought by the recipients of those materials. Now, in light of a recent, highly publicized New Jersey appeals court decision (*Doe v. XYZ Corp.*, New Jersey Superior Court Appellate Division, 2005), employers must also take heed that the scope of their potential liability has been expanded to third parties harmed by an employee when an employer knows—or has reason to know—that the employee is engaging in conduct that is potentially harmful and yet fails to take action in response to that information.

In the New Jersey case, an employee's spouse sued for damages on behalf of her 10-year-old daughter after an employee

was arrested for secretly videotaping and photographing the child in nude and seminude positions. Because the employee had used a computer belonging to the employer to repeatedly access pornographic Web pages—including pages containing child pornography—and to illegally upload and transmit explicit photos of his stepdaughter over the Internet, the wife claimed in her lawsuit that the employer had neglected its duty to report to the “proper authorities . . . crimes committed on its property during the course of the workday.”

Reversing the trial court, the appeals court noted that the employer had received several complaints about the employee's suspected viewing of pornography in the workplace as early as two years before the employee's arrest and, on at least one occasion, had uncovered evidence suggesting that the employee may have been accessing child pornography. Despite these complaints, the company had performed only a cursory investigation (rather than a thorough review of the Web pages accessed) and mildly admonished the employee to stop. In fact, the employer had failed to impose any other disciplinary measures—even after discovering that the employee later resumed this conduct—even though it had the capability to electronically monitor the employee's Internet activities as well as established workplace policies so that there was no legitimate expectation of privacy on the employer's computers.

Although the appeals court remanded the case to the trial court to decide if the wife could prove a connection between the employer's negligence and harm to the child, the case nevertheless shows that an employer has to investigate if it thinks an employee is using a workplace computer to access child porn. It also shows that an employer in this situation has to take prompt remedial action, including terminating the employee's Internet access and reporting the conduct to law enforcement authorities.

At least one state, New York, has proposed legislation which would require private employers and their information technology employees who observe or have knowledge that an employee is viewing child pornography to report the employee to the police.

Legal commentators nationwide have noted the opinion and

the potential trend for increased employer liability. At least one proposed state statute would also require private employers and their IT employees who discover an employee viewing child pornography to report the employee to the police. Several state statutes also require “computer technicians” to report suspected violations of child pornography laws.

### **GOVERNING EMPLOYEE CONDUCT**

In the face of such potential liabilities, what are corporate counsel to do? First and foremost, prudent employers should publish policies which put employees on notice that the company’s information and technology systems are to be used for business-related purposes only and that any conduct that violates the law or the firm’s nonharassment and other policies is strictly prohibited. Company policies should also clearly advise employees that all company-provided equipment—and the information stored on them—belong to the company and may be reviewed or monitored from time to time by management.

Further, company policies should include notice that abuse of the company’s information technology systems will result in disciplinary action (including termination), that the company will report any suspected illegal activities uncovered through its monitoring to legal authorities, and that the company will cooperate with law enforcement officials seeking evidence of illegal activities. Such written communications not only instruct employees on acceptable workplace conduct but also inform those individuals that they have no reasonable expectation of privacy in their communications made through company-owned devices and other equipment.

At a minimum, corporate information technology policies should be disseminated in an employee handbook and also posted in an accessible location (such as on a bulletin board in an employee break room). A company should also review its policy annually for necessary changes due to evolving technology. It may also want to consider redistributing its policy on a regular basis.

With each policy distribution, employees should be required to sign and return an acknowledgment form stating that they read, understood, and will comply with the policy. On a related note, employers should require that employees provide passwords for their devices (to reinforce the message that password protection does not preclude management’s access to this information) and consider instituting training programs on appropriate etiquette in e-mails, business-related research on the Internet, and participation in permitted company blogs.

Prudent employers should also prepare and enforce document-retention and computer-monitoring practices, the exact scope of which would depend upon the nature of the company’s business and applicable law. Software programs can aid employers in monitoring and tracking employee computer use and electronic communications, as well as set firewalls limiting the flow of certain types of data through screening e-mails and other communications for keywords. Before implementing such practices, employers should carefully weigh any negative impact on employees—such as increased stress and job dissatisfaction—as well as the potential for unintended side effects of screening programs (for instance, the risk that automatic blocking of sex-

based references in e-mails will interfere with the process of reporting harassment claims to human resources managers). Moreover, employers must make sure that they don’t run afoul of federal and state wiretapping statutes, electronic communications privacy acts, or spyware laws in their monitoring activities—particularly when corporate offices operate in multiple jurisdictions.

It is equally important that cautious employers establish complaint procedures and other investigatory processes to respond to any suspicions of abuse of the company’s technology systems in a timely and even-handed manner. The procedures should also preserve electronic materials and information when necessary for an investigation, when mandated by law, or in the face of litigation. Company procedures should include interim measures—such as removing an employee from Internet access at work—that will be imposed during the course of an investigation.

A process should also be established for communicating information to appropriate law enforcement officers if employers determine that unlawful conduct has occurred through the use of the employer’s information technology systems. Indeed, in the event any suspected illegal activities are uncovered, a company should determine its own obligations—whether imposed through the common law or applicable civil and criminal statutes—to potential third parties who may be harmed by the employee’s conduct.

Once an employee is suspected of abusing workplace technology and an investigation begins, the question becomes: How does the company ensure that it has a solid case and can withstand assertions of liability against the company by the employee or third parties? Computer forensics may be the key to uncovering evidence of wrongdoing, as it can provide information about when a document was created, who created it, who received it, and even what other documents the employee in question created.

Computer-forensic examiners are not simply limited to examining traditional desktop or laptop computers but may be able to unlock evidence of unlawful activities on other portable devices, such as cell phones, and virtually any devices capable of electronic storage. Through application of their practical experience, certification, and training, these examiners use forensic software to preserve and recover electronic evidence.

So what do you need to know as a corporate counsel to assist the examiner? First, understand that every keystroke of a computer can change evidence. Even the “power down” process can change data. Forget everything you have learned about safely “powering down” a computer, and never let the company’s IT technician just “take a look around” for evidence. To reliably preserve evidence, allow the electronic device’s battery to expire or remove the power cord from the computer. Store the device in a secure, climate-controlled environment away from any items, such as magnets or other computers, that might transmit signals that could affect the evidence. By not touching a button on the device, you won’t risk altering the evidence, and a trained examiner can still recover the information.

A thorough forensic examination may take several weeks. Even information that has been “wiped” may be recoverable.

Deleted information often still exists in some recognizable form on a system, even if it is not visible during normal operations. In the unlikely event that the evidence truly is nonrecoverable, the examiner may still be able to provide valuable information about the efforts the employee took to cover his tracks.

### **THE CYBERTIPLINE**

What if the examiner turns up not just adult pornography but also unlawful child pornography on an employee's computer? What if you find such images and can't tell if they are of children? You now face the dilemma of whether to risk wrongfully reporting an employee to the police if those in the pictures are, in fact, adults. Fortunately, there is a solution. If you submit a report of suspected child exploitation to the CyberTipLine, the National Center for Missing & Exploited Children will work with law enforcement personnel to review the images and determine whether they match other known images of child pornography.

Reporting to the CyberTipLine enables a company to have a permanent record of its efforts to contact law enforcement about concerns without rushing to conclusions about an employee's

activities when the evidence is unclear. If the images are determined to be child pornography, a law enforcement agency can then help the company handle the material appropriately.

Remember, too, that the upcoming changes to the Federal Rules of Civil Procedure require that parties be more knowledgeable sooner about potentially relevant electronically stored information. These new guidelines will have a significant effect on a company's duty to preserve and provide electronic discovery to opposing counsel if there is a lawsuit, and they should help shape employer policies and procedures on record retention, preservation, and backup on information technology systems.

Abuse of workplace technology is a serious concern for corporate counsel, and it is likely to be an increasing challenge as technology used by businesses develops and changes. This is an issue that corporate counsel must effectively confront.

---

*Adam P. Palmer is director of the office of legal counsel at the National Center for Missing & Exploited Children, based in Alexandria, Va. Sherri A. Affrunti is a partner in Reed Smith's labor and employment group, based in the firm's New Jersey office.*