Journal of Business Research 62 (2009) 1335–1341

Contents lists available at ScienceDirect

Journal of Business Research

Detours and frolics on the Internet: Employer liability and management control of cybertorts

Robert J. Aalberts [a,*], David S. Hames [b,1], Paul D. Thistle [a,2]

[a] Department of Finance, University of Nevada, Las Vegas, 4505 Maryland Parkway, Las Vegas, NV 89154-6008, United States
[b] Department of Management, University of Nevada, Las Vegas, 4505 Maryland Parkway, Las Vegas, NV 89154-6009, United States

ARTICLE INFO

Article history:
Received 20 April 2008
Accepted 18 December 2008

Keywords:
Electronic monitoring
Information technology
Risk management
Public policy
Organizational justice

ABSTRACT

Most employers are aware of their legal right to monitor employees' computer activities, and they are increasingly doing so. Yet, few of those who do monitor are aware that exercising this right may impose a legal duty to monitor prudently in order to protect third parties and to report criminal activity to the appropriate authorities. This paper briefly examines employers' legal right to monitor their employees' computer activities. Our subsequent analysis of the ruling in *Doe v. XYC Corp.* [Doe v XYC Corp., 382 N.J. Super. 122, 887 A.2d 1156 (2005)]. illustrates that those businesses that do assert their rights to monitor may assume a duty to report child pornography to the authorities, as well as a duty of reasonable care when reacting to their employees engaging in so-called cybertorts. We discuss how this ruling may extend the doctrines of 'detours' and 'frolics' into cyberspace. We also discuss the potential for employers' liability for other cybercrimes and cybertorts committed by their employees. We conclude by examining the contours of computer monitoring policies that effectively serve employers' risk management objectives without unduly invading employees' privacy, and the likely consequences of failing to achieve such a balance.

Most employers are aware of their legal right to monitor their employees' computer activities (Sotto and McCarthy, 2006), and they are increasingly doing so. Yet, few businesses are aware that when exercising this legal right they may owe a reciprocal legal duty to monitor their employees prudently in order to protect third parties and to report certain criminal activity to the appropriate authorities. The foundation for this emerging duty was illustrated recently in a New Jersey decision, Doe v. XYC Corp (2005). This case of first impression has triggered substantial debate throughout both the legal and business communities over the best way to balance the privacy rights of employees and the rights of third parties who may be harmed by employees' workplace Internet activities (Filisko, 2006; Gunnarsson, 2006; Stephenson, 2006).

This paper briefly examines employers' legal right to monitor their employees' computer activities. Our subsequent analysis of the ruling in *Doe* explains how the case may create a legal duty to monitor prudently in order to avoid "cyberfrolics." We discuss how this legal duty may extend the common law doctrines of 'detours' and 'frolics' into cyberspace. We also discuss employers' potential liability for other cybercrimes and cybertorts committed by their employees. We conclude by examining the contours of computer monitoring policies that effectively serve employers' risk management objectives without unduly invading employees' privacy, and the likely consequences if such a balance is not achieved.

1. The legal right to monitor

Employers are increasingly monitoring their employees' computer use. Surveys indicate that in 2001, 82% of employers were monitoring their employees' computer activities; by 2003, 93% were doing so. Similarly, employer spending on software that enables monitoring increased from $299 million in 2005 to $350 million in 2006, and is expected to exceed $600 million by 2010 (Vara, 2007; Center for Business Ethics, 2003; American Management Association, 2001). Companies have good reason to monitor. Pornography accounts for 35% of all downloads and 8% of all e-mails. Twenty percent of men and 13% of women admit to accessing porn at work. Half of Fortune 500 companies have had at least one incident of inappropriate images discovered in the workplace. Eighty-five percent of these led to disciplinary action. Twenty-six percent of companies have terminated workers for misuse of the Internet and another 25% have terminated workers for misuse of e-mail (Family Safe Media, 2007; Delta Consulting, 2005; American Management Association, 2003). Pornography is but one reason employers are increasing their monitoring of employees' computer use. Gambling, hateful, violent or otherwise tasteless activities have

* Corresponding author. Tel.: +1 702 895 3919.
E-mail addresses: robert.aalberts@unlv.edu (R.J. Aalberts), david.hames@unlv.edu (D.S. Hames), paul.thistle@unlv.edu (P.D. Thistle).
[1] Tel.: +1 702 895 3675.
[2] Tel.: +1 702 895 3856.

0148-2963/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jbusres.2008.12.005

contributed. The growing popularity of social networking sites has also raised concerns about sexual harassment, lost productivity, preserving bandwidth and security breaches (Vara, 2007).

Although such monitoring engenders concerns regarding employee privacy, employers' legal right to monitor is well established. The federal law most often cited for regulating electronic monitoring is the Electronic Communications Privacy Act (ECPA) of 1986. Under the ECPA, an employer cannot intentionally intercept and then disclose e-mails that are in transit. Moreover, the Stored Communications Act (SCA), which amended the ECPA, prohibits employers from intentionally disclosing stored e-mails. The ECPA, however, is riddled with exceptions. For example, an employer and its agents may intercept and disclose communications in the "ordinary course of business" when it is necessarily related to its business and to the protection of property as an Internet service provider (ISP). Thus, an employer may monitor unauthorized, company-related activities that may affect employee efficiency and profitability. Although the "ordinary course of business" is not defined in the ECPA, it generally will require that the monitoring be for a legitimate business purpose, be routine and with notice (see, e.g., Adams v. City of Battle Creek, 2001).

The ECPA also provides virtual immunity to employers when they are the providers of the electronic communications service. In Fraser v. Nationwide Mutual Insurance Co. (2003), for example, a federal circuit court ruled that the Company's search of an employee's e-mail that was stored in its system was exempt from the Act's protections. Since most searches are not executed contemporaneously with the time the e-mail is sent, but generally take place when the information is in storage, this provision provides employers with a particularly strong right to control and manage their employees' activities (Sampson, 2006).

Quite possibly the most important ECPA exception is when the employee gives prior consent to be monitored. Under the ECPA a company may adopt a Computer Use Policy and Agreement. If this policy and agreement is properly executed between employers and employees, and is consistently enforced, it will serve as notice to employees that their privacy rights are limited to what is provided for in the agreement. Even if employees are not asked to agree expressly to the policy, its existence may give rise to an employee's constructive knowledge of the policy if it is in writing, is consistently enforced, and the employee's actions constitute a flagrant violation of a universal standard of behavior (Autoliv ASP., Inc. v. Department of Workforce Services, 2001).

States, under both their statutory and common law, could limit employers' right to monitor by granting rights greater (but generally not less) than what is conferred under federal law. However, few states have exercised their rights to do so. For example, Connecticut and Delaware have enacted statutes granting employees protection against computer monitoring. These statutes both require employers to give employees advance notice if they are going to engage in electronic monitoring in the workplace (Sotto and McCarthy, 2006).

Employees have raised the common law right to privacy in an attempt to limit their employers' right to monitor, but they have not generally prevailed. One strand of the common law right of privacy occurs when someone intentionally intrudes upon an employee's solitude in his private affairs or concerns. To prevail under this cause of action, employees must show that they have a "reasonable expectation of privacy" in the workplace when using their employers' computers. Since employers have a legitimate interest in monitoring their employees' computer usage through its electronic communications service – property the employer owns and maintains – the courts have generally ruled that an employer's monitoring activities would have to invade areas that are "intensely private" before the employee's expectation of privacy could be considered reasonable (Sotto and McCarthy, 2006; Gabel and Mansfield, 2003). Thus, if the employer's motive was clearly non-business related, such as eavesdropping and closely monitoring personal messages with the intention of embarrassing the employee, the employee might be able to prevail. Employees may also enjoy more privacy rights on their company computers if they are sending e-mails through a personal e-mail account, such as Hotmail, which they access with their own private password. Because these e-mails are not stored on a company-owned service and a password limits access to it, the employee reasonably has a greater expectation of privacy. In either case, however, employees would waive their privacy rights if they consent to being monitored pursuant to a company policy (see, e.g., Fisher v. Mt. Olive Lutheran Church, 2002).

2. The case establishing a duty to monitor prudently: *Doe v XYC Corp*

While employers have a well-established right to monitor, the *Doe* case may create a duty for employers who do monitor employees' computer use to do so prudently. The compelling facts in *Doe* help to illustrate how the duty to monitor must be executed if a business is to avoid expensive, embarrassing and potentially destructive lawsuits. XYC Corporation employed 250 people, including "John," the plaintiff's then husband. John worked in an open cubicle near a corporate officers' corner office. XYC had a policy stating that e-mails were property of the company and that misuse of the Internet was to be reported to the Personnel Department. The company knew that John was married and had a young stepchild.

John's coworkers informed their manager that John was accessing and viewing pornographic sites on his company computer. In response, the company's Senior Network Administrator (SNA) checked John's computer logs, revealing that the complaints were apparently true. Indeed, some of the sites on the logs possessed highly suspicious and provocative names such as "bestiality" and "necrophilia." The SNA confronted John and ordered him to stop visiting "inappropriate sites" but did not inform John's supervisors.

About a year later, the SNA and John's immediate supervisor investigated again and found evidence of more provocative sites but did not actually view them. They requested that the Director of the Network and PC Services (Director) conduct an investigation. The Director, however, admonished the SNA, told him never to access employees' Internet activities, that it violated company policy to monitor Internet use, and threatened to fire the SNA. As a consequence, John was not told this time about the SNA's discoveries and he continued to access the illicit sites.

John's coworkers lodged additional complaints after catching him shielding his computer and quickly minimizing images, as well as leaving provocative images on his screen. Finally, John's immediate supervisor entered his cubicle while he was at lunch and clicked on John's "websites visited." He discovered a number of pornographic sites, including apparent child pornography sites. The supervisor, with permission from his superiors, told John to quit his illicit Internet activities, but took no further action. John agreed to this request, yet continued accessing the pornographic sites. In the end, the police, who had now been alerted by company supervisors, found nude photographs of John's 10 year old stepdaughter in the company dumpster. These were the same pictures that he had sent out as "payment" for access to the child pornography sites. The discovery of the pictures formed the basis for a search warrant of his office and computer in which an additional seventy downloaded pictures were discovered, including more pictures of his stepdaughter.

When John's actions were eventually made public, his now divorced wife sued XYC Company for failure to investigate and protect her daughter, including the harm she suffered from John. The trial court initially sided with the defendant in a motion for summary judgment; however the appellate court overruled it stating: "… [the] defendant had a duty to report Employee's activities to the proper authorities and to take effective internal action to stop those activities….Defendant was under a duty to exercise reasonable care to stop Employee's activities, specifically his viewing of child pornography which by its very nature