Information & Communications Technology Law
Vol. 19, No. 1, March 2010, 87–99

Routledge
Taylor & Francis Group

Electronic surveillance of Internet access in the American workplace: implications for management

Marian K. Riedy* and Joseph H. Wen

The School of Business, Emporia State University, Emporia, Kansas 66801, USA

Software that enables sophisticated and comprehensive electronic surveillance of employee Internet access is widely used by American businesses. No federal or state statute prohibits private employers from monitoring their employees' email or the websites they access. Corporate managers opt for surveillance to protect their corporations from legal exposure arising from employee misconduct, such as downloading or emailing pornographic material; to protect against the improper disclosure of proprietary information over the Internet; and because surveillance software is inexpensive. While the reasons offered by employers for conducting electronic surveillance may be valid, there are competing considerations. This paper reviews surveillance technologies, discusses arguments for utilizing electronic surveillance, and concludes with legal issues arising from surveillance and implications for management.

Keywords: electronic surveillance; technology; Internet access; privacy; productivity; liability

Introduction

Companies provide comprehensive Internet access to employees – via desktop and laptop computers, cell phones and personal digital assistants provided by the employer – to enhance productivity. Access to the Internet is an indispensable tool for quickly and efficiently communicating with people in remote corners of the globe, sharing a wealth of resources and ideas, and locating immense amounts of reference and resource materials. At the same time, this ready access to the Internet by company employees poses new challenges to management in the American workplace. The most critical issues include: (1) potential corporate liability for employee misconduct via the Internet; (2) diminished employee productivity from recreational use of the Internet; and (3) the unauthorized disclosure of proprietary information (Lee & Kleiner, 2003; Turri et al., 2008). Electronic surveillance of Internet access and usage has become a common method of addressing these issues.

Electronic surveillance is the use of computerized systems to automatically collect, store, analyze, and report information about employee behavior. Employers use many methods of electronic surveillance in the workplace today. For example, workers may be videotaped, tracked with RFID or GPS technologies, and have their telephone calls analyzed by a computer (Persson & Hansson, 2003). Employee

*Corresponding author. Email: mriedy@emporia.edu

ISSN 1360-0834 print/ISSN 1469-8404 online

DOI: 10.1080/13600831003726374
http://www.informaworld.com

surveillance is nothing new, but electronic surveillance differs significantly from traditional surveillance in at least two respects: (1) electronic surveillance makes it possible to monitor many employees simultaneously and to obtain much more detailed information; and (2) while formerly, people usually knew when the boss was there, electronic surveillance can be 'there' all the time.

Electronic surveillance of Internet access, in particular, is a common practice today. In 2005, an American Management Association (AMA) survey found that 76% of companies monitor connections to websites by employees, 65% block inappropriate websites using URL blocking software, and 55% retain and review email messages (AMA, 2005.) This widespread surveillance has real consequences for employees. In its survey, the AMA found that approximately 26% of companies have fired workers for misusing the Internet, 25% have fired employees for misusing email, and 6% have fired employees for misusing office telephones (AMA, 2005). Another consequence for employees is the loss of privacy entailed by widespread electronic surveillance. Scholars (Persson & Hansson, 2003) and advocacy organizations (American Civil Liberties Union, 1997) express concerns about this invasion of employee privacy interests.

What manner of electronic surveillance should a company employ in order to address the issues raised by employee Internet access in a way that is productive, cost effective, and legal? Many organizations are struggling with this question. This paper discusses electronic surveillance technologies and studies the rationale behind a corporate surveillance policy. This paper also reviews related legal cases and liability concerns raised by electronic surveillance and implications for management.

Surveillance technology

Surveillance software can track employees' Internet movements and prepare reports to management. As employees surf and browse the Web, those movements are actively monitored and reports generated, including real-time, online notification to the administrator of selected 'hits'. The technology is capable of taking a picture of an employee's computer screen at periodic intervals, enabling the employer to see the sites employees are visiting or the messages they are emailing. Surveillance technologies can screen employees' email for potentially offensive or inappropriate messages by scanning for questionable keywords pre-determined by the employer. For example, an employer concerned with the theft of its trade secrets can list the names of its primary competitors as keywords. The surveillance system can also automatically email 'flagged' messages to the employer. The capabilities of surveillance technology are described in Table 1 (Wen et al., 2007).

Electronic surveillance supported by increasingly sophisticated technology is here to stay, and it is a powerful tool for employers. However, how to use this tool to monitor employees' Internet access in the workplace most effectively is an open question. In the following section, the strengths of the arguments for and against electronic surveillance are discussed, in order to elucidate answers.

The arguments

Employers justify electronic surveillance of employee Internet access as promoting sound business interests. Yet the practice also raises concerns from all areas of society – business organizations, employee interest groups, privacy advocates, civil

Table 1. Electronic surveillance technology.

Surveillance capability	Description
Keystroke monitoring	• Maintains a record of keystrokes along with the window they are typed in and time stamp. • Tracks computer idle time. • Recreates 'deleted' documents because the keystrokes are logged and stored even if deleted.
Emails sent and received	• Monitors and logs all emails sent and received by users of all company owned computers. • Screens emails for potentially offensive or inappropriate messages. • Scans employee emails for questionable keywords pre-determined by the employer.
Events timeline logging	• Logs all events users performed and view them in an organized chronically ordered listing. • Views what the events the user performed, in the order they did them. • Logs program starts/stops, website visits, document viewings and printings.
Application usage	• Monitors and logs all applications run by users. • Logs when the application was started, stopped, and how long it was actually used. • Records application installations performed by users. • Logs software name, installation path, and time when installation is logged.
Window activity	• Records documents and files opened and viewed by users. • Logs all windows in which the user directly interacts on the desktop. • Monitors and logs all Internet sessions and all chat conversations made on the PC. • Records documents and files that are printed by users. • Logs all passwords used during monitoring sessions via its keystrokes recorder.
Remote desktop viewing	• Takes snapshots of every desktop at set intervals of time, allowing managers to visually see what is happening. • Views a listing of various system information for the remote PC, including processor type, system directory. • Views a list of the current Internet connections on the PC. • Views a list of the recent documents users have opened. • Remotely views what the user is doing in real time.

Source: Wen et al. (2007).

libertarians, lawyers, and professional ethicists. Each advocate advances economic, legal, and ethical rationales in support of their position. However, no argument is conclusive and each raises important managerial and moral issues.

Liability

The primary reason cited by employers for conducting electronic surveillance is to minimize legal liability arising from employee misconduct: harassing email and illegal downloading, for example (Porter & Griffaton, 2003). But surveillance is at best a two-edged sword in this regard. To the extent that surveillance and monitoring deter employee misconduct, employer liability is reduced. The same is true if

surveillance accomplishes early detection and response, such that misconduct is identified and stopped before it becomes actionable.

However, electronic surveillance also simply accumulates data. Many companies retain business records, including electronically stored information, for some period of time as dictated by law or in order to promote business management and planning purposes. Others automatically archive and retain data because they do not have a document retention and destruction policy in place (ePolicy Institute, 2004). Extensive surveillance coupled with data retention increases the likelihood that evidence of employee wrongdoing via Internet access is in the company's custody or possession. If that evidence is discovered by an opposing party, the company has, because of its surveillance, increased the likelihood of being found liable for that misconduct.

Productivity

A second justification for surveillance of Internet access is to reduce non-business use of the Internet (Turri et al., 2008). When employees surf the Internet and send personal email they are using company resources for unproductive purposes and reducing time spent doing the job, as the reasoning goes. Surveys indicate that personal or recreational Internet access is common. For example, a 2004 survey found that 85% of employees engaged in personal email while on the job (ePolicy Institute, 2004). The Internet may have usurped gossiping in the coffee room or talking on the telephone as the leading employee diversion from work.

However, there is no definite evidence that employee productivity, as a whole, has decreased because employees are forwarding email to colleagues instead of meeting them in the coffee room. Indeed, email could be quicker, reducing the amount of employee time spent on personal matters. If surveillance of employee Internet access deters personal use of the Internet – another unproven assumption – the result may be counterproductive. Employees who would book a flight on line have to leave the office to go to a travel agent.

Even if surveillance deters employees' recreational use of the Internet, the fact of surveillance alone may otherwise adversely affect productivity. 'When workers begin to feel that their employer does not trust them, their mental well-being is harmfully impacted' (Wen et al., 2007). The exact effect of employee surveillance is uncertain because little research has been done on separating the effects of surveillance from job design, equipment design, lighting, machine pacing, and other potentially stressful aspects of a computer-based office worker. Early studies showed that working under surveillance provides a source of worry for workers. More recent studies indicate that employees feel electronic surveillance is beneficial, or at least necessary (Allen et al., 2007). But an environment of surveillance may unknowingly curtail otherwise productive activity, as employees act and then think in response to the unseen observer. New, radical, unconventional ideas may be filtered out of communications if the employee is constantly worried what the observer may think. But corporations rely upon creative, new thinking in order to constantly move forward and improve. In fact, most companies work hard to form innovative and open teams to foster creative employees and improved products and services. Innovation comes only from creativity and, it is argued, is in jeopardy when that creativity is stifled with even the threat of surveillance.

A separate but related issue arises from the fact that employers must devote resources to managing the surveillance itself. As surveillance technologies become increasingly complex, even more resources must be devoted to interpreting the data that is collected (Brian, 2008). The extent to which employee Internet access should be monitored in order to increase productivity should be determined to some extent by the true costs of conducting and responding appropriately to that surveillance.

Security

With a greater reliance on computer systems, information assets are seen as a vulnerable point of attack by would-be saboteurs. Corporations that do not adequately secure their systems risk unwanted dissemination, retrieval, or modification of private corporate information. Proponents argue that monitoring employees protects the safety and security of the organization and even the nation. In addition, disloyal employees are able to email trade secrets and confidential documents quickly and easily to a large audience. In fact, most security breaches come from knowledgeable insiders – not random hackers from the outside (Wakefield, 2004). By monitoring Internet usage and content, corporations argue that they are able to detect and halt security breaches.

Securing confidential and proprietary information from unauthorized access from outside, and prohibiting unauthorized and illegal disclosure by employees is inarguably a legitimate objective. Whether or not surveillance of employee Internet usage accomplishes these objectives is unclear. Certainly a company would have to update its surveillance technology in order successfully to combat a hacker or disloyal employee using the most sophisticated detection-avoidance software.

Ethical issues and fairness

Electronic surveillance offers a distinct advantage to the employee: it is objective. This is a benefit because it provides an unbiased method of monitoring employee Internet access; managers are not picking and choosing which employees to monitor.

Electronic surveillance may be objective and unbiased, but it also invades employees' privacy. To what extent employees have a *right* to privacy in the workplace is a matter of considerable debate (Lasprogata et al., 2004; Persson & Hansson, 2003). However, most commentators would agree on certain parameters. Employers are entitled to conduct electronic surveillance of employees in order to meet the legitimate objectives discussed above (Persson & Hansson, 2003). But if the employer's surveillance practices are seen as unduly intrusive (Allen et al., 2007), excessively controlling (Allen et al., 2007), or employed for no legitimate business objective (Persson & Hansson, 2003), those practices may be viewed as unethical. The practical effect of surveillance practices viewed as unfair may be a loss of productivity or employee resignations.

Legal and managerial implications of electronic surveillance

It is by now well established and widely known that a private employer can conduct electronic surveillance of its employees' Internet access without running athwart of

the law.[1] The various potential barriers to these practices raised in claims brought by employees affronted by surveillance – including prohibitions on the interception of electronic communications in Title I of the Electronic Communications Privacy Act ('ECPA'), 18 U.S.C. §§ 2501–21, restrictions on accessing stored electronic communications in Title II of the ECPA (the 'Stored Communications Act' or 'SCA'), 18 U.S.C. §§ 2701–11; and common law remedies for invasion of privacy and similar torts – are too porous to prevent electronic surveillance, for reasons that need not be repeated in detail here (Nord et al., 2006).

Though as a general matter neither federal nor state law precludes surveillance,[2] an employer does not, of course, have *carte blanche* to monitor an employee's electronic communications. Further, once an employer undertakes electronic surveillance, it may be exposed to liability not because of the surveillance *per se*, but as a consequence of it. As set forth below, the case law reveals pitfalls to avoid, and issues to consider, even in this era when, in general, employees are accustomed to surveillance.

Privacy rights still exist

In the common law of torts, an 'invasion of privacy' ordinarily has two elements: the defendant must have intentionally intruded into a place, conversation, or matter as to which the plaintiff has a 'reasonable expectation of privacy', and the intrusion must occur in a manner 'highly offensive to a reasonable person'.[3] An invasion of privacy claim arising in the workplace typically fails because the employee is (because of explicit notification given by the employer) or should be on notice that the employer owns and therefore can access and control 'company property' and 'company equipment', including computers. Hence, an employee has no 'reasonable' expectation of privacy in email sent on the employer's system or in a URL accessed by a company computer.[4]

Nonetheless, the company cannot declare all property 'subject to surveillance' without consequences. When electronic surveillance was in its relative infancy, several cases made headlines – and resulted in damages awards to plaintiffs – because of the 'inherently private' nature of the location being monitored. For example, in *Doe by Doe v. B.P.S. Guard Services Inc.*, 945 F.2d 1442 (8th Cir. 1991), the court held that the employees – models at a fashion show – had a reasonable expectation of privacy in curtained changing areas, and the secret viewing and videotaping of them while changing constituted a tort. Based on similar facts, the plaintiffs succeeded in establishing an invasion of privacy claim in *Liberti v. Walt Disney World Co.*, 912 F. Supp. 1494 (M.D. Fla. 1995). A similar but more recent case is *Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094 (C.D. Cal. 2006), in which the court ruled in favor of the employees' common law and constitutional violation of privacy claims when they were secretly videotaped undressing in locker rooms in the basement of their place of work.

But the specific location under surveillance need not be 'inherently private', like a changing room or bathroom, to justify an employee's reasonable expectation of privacy in that location, including a computer in that location. For example, in *Hernandez et al. v. Hillsides Inc.*, (47 Cal. 4th 272, 47 Cal. Rptr. 1063, 2009), employees of a residential facility for neglected and abused children brought invasion of privacy and other claims against the employer for installing a hidden camera in their office to record websites accessed on the computer in the office.

The facts showed that the office had a door that could be locked and shades to be drawn, and was provided

> . . . to allow the occupants to obtain some measure of refuge, to focus on their work, and to escape visual and aural interruptions from other sources, including their employer. Such a protective setting generates legitimate expectations that not all activities performed behind closed doors would be clerical and work related.

Further, though the employer had an explicit policy advising employees that their email and Internet usage would be monitored, that policy

> . . . is distinguishable from and does not necessarily create a social norm that in order to advance that same interest, a camera would be placed inside their office, and would be aimed toward a computer workstation to capture all human activity occurring there. (47 Cal. 4th 272 at 294)

The California appellate court held that the employees did have a reasonable expectation of privacy.

The *Hernandez* court went on to find that the evidence did not support the second leg of the tort: the invasion of privacy was not 'highly offensive to a reasonable person' largely because the employer had a legitimate reason for the surveillance. The camera was installed after the director of the facility learned that late at night, after the plaintiffs had left the premises, an unknown person had repeatedly used a computer in the plaintiffs' office to access the Internet and view pornographic websites. Further, the employer had limited the invasiveness of the surveillance by taping only during the night when the employees were not using the office.

Even surveillance of an 'open to the public' space can wrongfully invade privacy interests. In *Bowyer v. Hi-Lad, Inc.*, 216 W. Va. 634 (2004), the West Virginia Supreme Court upheld a jury verdict in favor of a hotel employee whose conversations with clients as they were checking into the hotel were videotaped by a secret microphone. The employer had argued that an employee working at the front desk could have no 'reasonable' expectation of privacy, as a matter of law, but the court disagreed. 'Most employees, even those working in ''public'' spaces, have a reasonable expectation that their oral communications with other employees or with customers are not going to be recorded by hidden microphones.' [5]

It should be noted that invasion of privacy is but one of the common law remedies for allegedly improper surveillance. Liability can arise from the intentional infliction of extreme emotional distress, and, in some states, from the negligent infliction of extreme emotional distress. A plaintiff may also make claims under state constitutional rights to privacy. A few states, including Delaware, 19 Del. C. § 705 (2010), and Connecticut, Conn. Gen. Stat. § 31-48d (2008), by statute also require that advance notice of surveillance must be given by the employer, and a private right of action may lie for violation of that statute.[6]

For managers, these cases suggest that if Internet access from computers in locations that are arguably 'inherently private', or those that can be made private by the employee – places that have been constructed or set aside for semi-private use – is being monitored, management should be prepared with a justification. When the degree of surveillance is heightened – presumably because the surveillance has succeeded in its purposes of detecting possible problems – it should be done pursuant to standard operating procedures. That is, if the existing policy does not contemplate and include what procedures should be employed in the event of a targeted

investigation, it should be revised to do so. And those procedures should be designed on the assumption that the alleged culprit is innocent until proven guilty. If it were an innocent person, what type of surveillance would be considered reasonable and what not? Fewer complaints will arise – or succeed if they do arise – if the company has been completely fair in this regard.

Beware of monitoring private email accounts

To some extent, the battle lines have been redrawn. Because employees know their company email accounts will be monitored, they are using their own, private accounts, sometimes while on the job. Employers are well aware of this fact, and may attempt to access those private accounts, for the same reasons they monitor company accounts. Whether the employer can access and monitor these 'private' accounts depends upon what, if any, nexus there is to the place of work and/or the employer's computer equipment.

In *Thygeson v. U.S. Bancorp et al.*, 2004 U.S. Dist. LEXIS 18863 (D. Or. 2004), the facts showed that in the course of investigating an employee's use of the Internet for personal purposes, the employer had identified all the websites the employee had visited over a period of time, including the website he had used to access his Netscape email account. The employer had not actually accessed the email in the account. The employee sued for, inter alia, invasion of privacy, a claim the court rejected.[7] The court noted: 'In contrast to an e-mail system provided by an employer, most employees have a higher expectation of privacy when accessing personal Internet e-mail accounts, such as Netscape or Hotmail accounts, even when doing so while at work.' [8] However, the court concluded that the employee did not have a reasonable expectation of privacy when using the employer's computer and Internet access, at least so long as the employer collected only the website addresses, not the actual content of the email.

However, when the employee has not, or has rarely used a company computer to access a personal email account, the outcome may be different. In *Rozell v. Courtney Ross-Holst et al.*, 2007 U.S. Dist. LEXIS 46450 (S.D.N.Y. 2007), the plaintiff brought a claim under the ECPA, alleging that her employer's agent hacked into her AOL email account and stole sensitive information. The defendant moved for summary judgment on the grounds, inter alia, that the ECPA did not prohibit the 'authorized' interception of email and because the company owned the AOL account, the statute had not been violated.[9] But the court denied the motion, finding that the facts were in dispute: the plaintiff had originally opened the account, and her user name was on the account, and it was not clear what the licensing agreement provided insofar as access to the account was concerned. And though the employer argued that the plaintiff had implicitly authorized access to the account by using company computers to read her AOL email, the court found that this was a conclusion that rested on disputed issues of fact.

Similarly, in *Pure Power Boot Camp Inc. et al., v. Warrior Fitness Boot Camp et al.*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008), the employer brought various claims against its former employees including trademark infringement and breach of fiduciary duty. The employer sought to use as evidence a number of emails sent and received by one of the individual defendants, to which the defendants objected. The emails were in personal accounts, and had been drafted or received on the employee's home computer, though he had also viewed his personal email on company computers from time to time. The court agreed to exclude the email,

concluding that the employer had accessed the email without authorization, in what would have been a violation of the SCA had a cause of action been brought. In so holding, the court rejected the employer's argument that the employee had 'authorized' access to his email because he inadvertently left his username and password information stored on the company's computers, information the employer had used to enter the account.

For managers, these cases suggest that if the company is going to monitor an employee's access to personal email websites and/or access personal email in those accounts that fact should be made explicit in a published surveillance policy. And in regard to what usage will be allowed, consider that a blanket prohibition on accessing personal email accounts from a company computer might well prove counterproductive, and be seen as unfair. For example, would it be advisable to prohibit an employee who works virtually 24/7 because he or she carries a company-provided Blackberry from using that Blackberry to access personal email?

Be aware of responsibilities undertaken as a consequence of monitoring

Employers monitor employees' Internet access in order to collect, store, and analyze data for various purposes: to assess employee productivity, prevent security breaches, and to detect and/or prevent employee misconduct, or the abuse of email or Internet access. But the fact that the employer has collected and has access to certain data may by law impose responsibilities on that employer which, if not fulfilled, form the basis for liability.

An employer must act on improper employee conduct of which it 'knew or should have known'

Electronic surveillance of employee communications increases the probability that an employer knows, or should know, if employees are misusing the communication network. Although the employer might not have known or had reason to know of whispers in the hallway or even pornographic posters taped to a door, it may be harder to defend against an allegation that it had knowledge, or should have had knowledge, when its employee's communications are so often made electronically, and those electronic communications are under regular surveillance.

For example, a claim of a 'hostile work environment' under Title VII requires the plaintiff to show that a specific basis exists for imputing the alleged objectionable conduct to the employer. In the case of co-worker harassment, the employer will be liable if the employer is negligent, because the employer either (1) provided no reasonable avenue of complaint; or (2) knew, or should have known, about the harassment but took no action to stop it.[10] If, for example, the means of harassment is email, the substance is crude or pornographic language, and the employer is regularly monitoring email – and getting reports of 'hits' on crude or pornographic words – the 'knew or should have known' element has arguably been met, almost *per se*. The only remaining question would be whether the employer took prompt and reasonable steps to stop the harassment. If the surveillance is 24/7, and reports come in daily, the employer would likely be hard-pressed to claim that inaction for several months would be 'prompt and reasonable'.[11]

Another example arises from harm caused by an employee to a third party. A tort claim for negligent retention lies, and an employer can be *directly* liable for an

employee's intentional misconduct that causes harm to a third party, if the evidence shows that it 'knew, or had reason to know' of some dangerous propensity on the part of that employee but, nonetheless, kept him employed.[12] If an employee is sending threats or including violent language in email to a targeted victim, and harm ensues, an employer regularly monitoring email for such language might face a claim for negligent retention.

Surveillance may expand the net of vicarious liability

As is well known, an employer is vicariously liable for torts committed by an employee that are 'within the scope' of the employment. Several courts dealing with 'cyber torts' committed by employees have dismissed the derivative or *respondeat superior* action as against the employer because, more often than not, these are intentional torts which are as a general matter not 'within the scope of employment'.[13] For example, in *Booker v. GTE.Net LLC, d/b/a Verizon Internet Solutions et al.*, 214 F. Supp. 2d 746 (E.D. Ky. 2002), Verizon employees sent a nasty letter to a prospective client using the plaintiff's email account without her authorization or knowledge. She was investigated, and eventually exonerated, but sued Verizon for the emotional and psychological injuries caused by the incident, alleging that it was vicariously liable for the conduct of its employees.[14] Applying Kentucky law, the court noted that four factors are considered in determining whether an employer has vicarious liability: (1) whether the conduct was similar to that which the employee was hired to perform; (2) whether the action occurred substantially within the authorized spatial and temporal limits of the employment; (3) whether the action was in furtherance of the employer's business; and (4) whether the conduct, though unauthorized, was expectable in view of the employee's duties. Though the court deemed it a 'close call', it held that the factors tilted in Verizon's favor, largely because the conduct was clearly not in furtherance of Verizon's business.[15]

But in another case, another doctrine may come into play. Ratification is the adoption or confirmation by an employer of an act performed on its behalf by an employee which act was performed without authority. The doctrine of ratification is based upon the assumption that there has been no prior authority, but ratification by the employer of the employee's unauthorized act is equivalent to an original grant of authority. Upon acquiring knowledge of his employee's agent's unauthorized act, the employer must promptly repudiate the act; otherwise, it will be presumed that it has ratified and affirmed the act. An employer who learns or should have learned, through surveillance that an employee has committed an intentional tort that was not when committed within the scope of employment may be held to have ratified that tort if prompt action is not taken to repudiate the employee's conduct.

Surveillance may create duties to prevent harm caused by and to non-employees

Companies are accustomed to and therefore take the necessary steps to fulfill their responsibilities to provide a reasonably safe workplace for their employees, and to prevent harm caused by their employees to third parties. But one could imagine circumstances in which electronic surveillance would add a responsibility to prevent harm caused by and to non-employees.

Many companies monitor their networks to protect against security breaches: intrusions from outsiders. Suppose in the course of this surveillance a company intercepts communications from an outsider that indicates that person poses an imminent threat to another person or entity outside of the company. The company may have a duty to act to prevent that threat of harm because it has assumed the duty of that surveillance.

Most states have adopted the 'assumed duty' doctrine set forth in § 323 of the Restatement (Second) of Torts, or some version thereof. The Restatement provides:

> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of the other's person or things, is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking if
>
> (a) his failure to exercise such care increases the risk of such harm, or
> (b) the harm is suffered because of the other's reliance upon the undertaking.

If the facts showed that the company's inaction would somehow increase the risk that harm would result, or the innocent third party knew of and relied on the company's surveillance for his or her own safety, the company could be liable if harm does result pursuant to this doctrine of assumed duty.

For managers, these cases suggest that published surveillance policies describing how and when employees are going to be monitored are not sufficient. Protocols should be developed for prescribing how the data obtained from surveillance is going to be analyzed and how and by whom an appropriate response is determined and implemented.

Surveillance policies must be consistently applied and enforced

A typical surveillance policy advises employees something to the effect that 'all data created, transmitted, downloaded, or stored on the system is company property, and the company will monitor and record employee activity on its computers, network, and email systems, and websites accessed'. Both 'under' and 'over' enforcement of such a policy may present the employer with legal problems.

For example, in several cases the plaintiff alleged illegal retaliation arising from intensive or excessive electronic surveillance.[16] 'Retaliatory surveillance' claims pre-date the advent of electronic surveillance.[17] But it is presumably quicker and easier to 'up' the level of electronic surveillance – and easier for the plaintiff to obtain computer forensic evidence of such surveillance in discovery – than it was for the supervisor to peer over the wall into the employee's cubicle.

The opposite inconsistency is when the surveillance policy is generally under-enforced, but one employee is for some reason singled out for surveillance. In *Thygeson v. U.S. Bancorp et al.*,[18] the employee sued on the grounds that the employer had fired him in order to interfere with his acquisition of severance benefits, in violation of federal law. The employer argued that, to the contrary, Thygeson had been terminated 'for cause' for spending an inordinate amount of time on the Internet during work hours, which was detracting from his effectiveness as a manager, and downloading sexually inappropriate material on to his work computer, and moved for summary judgment on the claim. The court denied the motion, based on Thygeson's evidence of 'disparate treatment' in the application of the surveillance policy: basically, other employees had been warned but not

terminated because of excessive Internet usage, but Thygeson had been immediately terminated.

A general under-enforcement of a surveillance policy may resurrect an employee's 'reasonable expectation of privacy' in her electronic communications. The courts relied heavily on the fact that employees knew or should have known that they were being monitored in rejecting common law invasion of privacy claims. That an employer had an explicit policy on electronic surveillance also factored into the decisions holding that an employer's electronic surveillance did not violate the ECPA or SCA because the employee had implicitly 'consented' to that surveillance by receiving or signing the policy. If the employer knows that all of its employees regularly check their Facebook™ pages but does nothing, it may be hard-pressed to justify taking adverse action against any one employee for doing so, as in *Thygeson*, but also to successfully defend against an invasion of privacy claim.

For managers, these cases suggest that protocols should be developed for 'monitoring the monitor', to ensure that electronic surveillance isn't misused as 'retaliation' and that whatever surveillance policies are in place are consistently enforced.

Notes

1. We do not here consider limitations imposed on public employers by virtue of, inter alia, the Fourth Amendment prohibition against unreasonable searches and seizures.
2. One exception may be if the employees are unionized, because of statutory restrictions on employer interference with union activities.
3. See e.g. *Hernandez v. Hillside Inc.*, 47 Cal. 4th 272, 285, 47 Cal. Rptr. 1063 (2009). The precise definition of the tort varies somewhat by state, but the material elements are essentially the same.
4. The notice may explicitly state that employees have 'no reasonable expectation of privacy in any ... use of Company computers, network and system'. *Id.*, 47 Cal. 4th at 280.
5. *Id.* at 907.
6. Cf. *Vitka v. City of Bridgeport*, 2007 Conn. Super. LEXIS 3486 (2007).
7. Thygesen's other claims are discussed below.
8. 2004 U.S. Dist. LEXIS 18863, at *23.
9. The defendant also argued that the email had not been 'intercepted' within the meaning of the ECPA because the email was stored, not 'in transit'. We do not here delve into the judicial debate as to what constitutes the 'interception' within the meaning of Title I of the ECPA. See e.g. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004). But it should be noted in this context that email is either 'in transit' or stored, and Title II of the ECPA, the Stored Communications Act, prohibits unauthorized access to 'stored' email. See *Pure Power Boot Camp Inc. et al. v. Warrior Fitness Boot Camp et al.*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) for a discussion of the interplay between the two Titles.
10. E.g. *Richardson v. New York State Department of Correctional Service*, 180 F.3d 426, 441 (2d Cir. 1999), abrogated on other grounds, *Burlington Northern and Sante Fe Railway Co. v. White*, 126 Supreme Court 2405, 165 L. Ed. 2d 345 (2006); *Murray v. New York University College of Dentistry*, 57 F.3d 243, 249 (2d Cir. 1995).
11. Some commentators argue that under certain circumstances an employer which regularly monitors electronic communications should have enhanced responsibilities in regard to complying with Title VII: employers should be expected to detect and prevent the transmission of offensive electronic communications. Thus, '[e]mployers using blocking and monitoring technology have effective notice of potential workplace sexual harassment before the intended recipient receives it. As a result, the employers should bear the burden of providing reasonably sufficient technical protection to limit exposure to digital workplace sexual harassment' (Harris et al., 2005, p. 87).
12. E.g. *Kansas State Bank and Trust Co. v. Specialized Transportation Services Inc. et al.*, 249 Kan. 348, 819 P.2d 587 (1991).

13. But see e.g. *Charles Schwab & Co. v. Carter*, 2005 U.S. Dist. LEXIS 21348 (N.D. Ill. 2005), in which the court denied a motion to dismiss in which the defendants argued that appropriation of trade secrets was outside the scope of employment when the allegations were that the employer had 'urged' the unauthorized access to computer records in order to accomplish the appropriation.
14. The Booker court rejected the plaintiff's negligent supervision claim on the simple grounds that she had not alleged that Verizon knew or should have known that the offending employees would act as they did.
15. See also *Delfino v. Agilent Technologies Inc*., 145 Cal. App. 4th 790 (2006). The court's discussion of the derivative liability issue was technically dicta, as it found that Agilent was immune from liability for the 'publication' of the allegedly defamatory statements on the Internet pursuant to the Communications Decency Act.
16. See e.g. *Clinkscales v. Children's Hosp. of Phila*., 2007 U.S. Dist. LEXIS 83930, at *3, 4 (E.D. PA. 2007); *Zakrzewska v. New Sch*., 598 F. Supp. 2d 426, 436 (S.D.N.Y. 2009.)
17. See e.g. *Mattern v. Eastman Kodak Co*., 104 F. 3d 702 (5th Cir. 1997).
18. See *Thygeson v. U.S. Bancorp et al*., 2004 U.S. Dist. Lexis 18863.

References

Allen, M., Coopman, S., Hart, J., & Walker, K. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly: McQ*, *21*(2), 172–201.

AMA. (2005). *2005 electronic monitoring & surveillance survey: Many companies monitoring, recording, videotaping – and firing – employees* (2005 AMA survey, summary of key findings, May 2005). Retrieved from http://www.epolicyinstitute.com/survey2005summary.pdf

American Civil Liberties Union. (1997). *Privacy in America: Electronic monitoring*. Retrieved from http://www.aclu.org/technology-and-liberty/privacy-america-electronic-monitoring

Brien, M. (2008). Law, privacy, and information technology: A sleepwalk through the surveillance society? *Information & Communications Technology Law*, *17*, 25–35.

ePolicy Institute. (2004). *2004 workplace e-mail and instant messaging survey*. Retrieved from www.epolicyinstitute.com/survey/index.asp

Harris, D.P., Garrie, D.B., & Armstrong, M.J. (2005). Sexual harassment: Limiting the affirmative defense in the digital workplace. *University of Michigan Journal of Law Reform*, *39*, 73–98.

Lasprogata, G., King, N., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, *4*, 1–76.

Lee, S., & Kleiner, B. (2003). Electronic surveillance in the workplace. *Management Research News*, *26*(2–4), 72–82.

Nord, G., McCubbins, T., & Nord, J. (2006). E-monitoring in the workplace: Privacy, legislation, and surveillance software. *Communications of the ACM*, *49*(8), 73–77.

Persson, A., & Hansson, S. (2003). Privacy at work – ethical criteria. *Journal of Business Ethics*, *42*, 59–70.

Porter, W., & Griffaton, M. (2003). Between the devil and the deep blue sea: Monitoring the electronic workplace. *Defense Counsel Journal*, *70*(1), 65–78.

Turri, M., Mariam, B., & Hynes, G. (2008). Are they watching? Corporate surveillance of employees' technology use. *The Business Review, Cambridge*, *11*(2), 126–131.

Wakefield, R. (2004). Computer monitoring and surveillance. *The CPA Journal*, *74*(7), 52–59.

Worsnop, R. (1993). Privacy in the workplace. *CQ Researcher*, *3*(43), 1011–1025.

Wen, J., Schwieger, D., & Gershuny, P. (2007). Internet usage monitoring in the workplace: Its legal challenges and implementation strategies. *Information Systems Management*, *24*, 185–196.