Employee Responsibilities and Rights Journal, Vol. 15, No. 3, September 2003 (© 2003)

Electronic Monitoring to Promote National Security Impacts Workplace Privacy

Nancy J. King[1]

This paper explores electronic workplace monitoring in light of the USA PATRIOT Act—federal legislation with a national security focus that expands the likelihood of electronic workplace monitoring to assist government investigators. The paper examines federal laws that cover the privacy rights of at-will employees in the context of electronic workplace monitoring, including recent cases that have narrowed employee privacy rights. The paper argues that business justifications for electronic workplace monitoring have been bolstered by national security concerns, resulting in decreased expectations of privacy in the workplace for at-will employees. There are persuasive arguments that employers should exercise restraint in the use of information obtained through electronic monitoring in discipline and discharge decisions related to at-will employees. These arguments in favor of exercising restraint flow from the text of the USA PATRIOT Act and consider the risk of discrimination lawsuits.

KEY WORDS: electronic monitoring; at-will employment; privacy; national security; USA PATRIOT Act.

INTRODUCTION

Recent federal legislation designed to enhance national security expands the likelihood of electronic workplace monitoring (USA PATRIOT Act, 2001). From the perspective of employees, electronic workplace monitoring involves important privacy concerns because it allows employers to review employee communications, including e-mail and Internet activity (Rothstein, 2000). Employees argue their nonjob-related communications, including e-mail and other electronic communications made in the workplace using employer provided computer systems, are private and should not be monitored by employers (Rogers, 2002). From the employer's perspective, there are many good business reasons to electronically monitor employees in the workplace, including assessing worker productivity, protecting company assets from misappropriation, and ensuring compliance with workplace policies and nondiscrimination laws (Kane, 2001).

Recently, the business justifications for employer monitoring have been bolstered by their relationship to national security concerns (Evans, 2002). The ability of employers

[1]Department of Management, Marketing and International Business, College of Business, Oregon State University, 200 Bexell Hall, Corvallis, Oregon 97331-2603; e-mail: kingn@bus.oregonstate.edu.

0892-7545/03/0900-0127/0 © 2003 Plenum Publishing Corporation

to electronically monitor their computer systems and discover electronic evidence related to terrorism, computer hacking, and other crimes have an obvious relationship to national security. Although employers and employees have mutual interests in promoting national security, reduced expectations of privacy in the workplace significantly impact at-will employees as discussed in this paper.

The paper begins with an overview of the scope of electronic monitoring and the technology that has enhanced the ability of employers to monitor the workplace. The next section of the paper discusses the relationship between employee privacy and the at-will employment relationship, including the failure of state tort laws to restrain workplace monitoring. The third section of the paper discusses federal privacy statutes and electronic monitoring by employers, including recent cases that have applied federal privacy statutes to workplace monitoring and, in some cases, narrowed the scope of federal privacy protections. The fourth section of the paper discusses the impact of recent amendment to federal privacy laws by the USA PATRIOT Act, including the implications for employer electronic monitoring activities related to assisting government investigations of terrorism activities. The fifth section of the paper discusses privacy concerns shared by employers and employees, including concerns related to disclosures by Internet Service Providers under contract with employers and employees.

The last section of the paper analyzes the ways that electronic workplace monitoring to further national security interests has tipped the privacy balance in private-sector workplaces. This section advocates restraint by employers in electronic monitoring of the workplace and termination decisions based on electronic monitoring. The paper argues that there are good reasons for employers to exercise restraint in electronic workplace monitoring because it is consistent with the text and purpose of the USA PATRIOT Act, and it makes good business sense to minimize the likelihood of discrimination claims and expensive litigation.

TECHNOLOGY ENHANCES THE EMPLOYER'S ABILITY TO ELECTRONICALLY MONITOR THE WORKPLACE

Advances in computer technology have increased the employer's ability to monitor the electronic communications of employees in the workplace. It is estimated that over three quarters of major U.S. firms record and review employee communications and activities on the job, including telephone calls, e-mail, Internet connections, and computer files (American Management Survey, 2001).

Scope of Electronic Monitoring

The term electronic monitoring is used in this paper to encompass three different concepts. First, it includes employer use of electronic devices to review and measure the work performance of employees (Hébert, 2002). For example, an employer may use a computer to retrieve and review an employee's e-mail messages sent to and from customers in order to evaluate the employee's performance as a customer service representative. Second, it includes "electronic surveillance" by an employer using electronic devices to observe the actions of an employee for purposes other than measuring work performance (Hébert, 2002).

For example, an employer may electronically review an employee's e-mail messages as part of an investigation of a sexual harassment complaint. Electronic surveillance by an employer also includes electronic monitoring in compliance with a government order to search and seize electronic evidence, such as employer monitoring to comply with a search warrant seeking an employee's voice mail or e-mail communications on the employer's computer systems. Third, electronic monitoring includes employer use of computer forensics, the electronic recovery and reconstruction of electronic data after deletion, concealment, or attempted destruction of the data (Computer Forensics Defined, 2002; Leahy, 2002). For example, an employer may use specialized software to retrieve e-mail messages related to an investigation of alleged theft of its trade secrets by retrieving and reconstructing e-mail messages sent by an employee (the alleged thief) to someone outside the company.

Technology Used for Electronic Monitoring

There are many ways that employers may use computer technology to monitor the workplace. Employers may monitor employees' use of computer keyboards. It is possible to program computers to monitor clerical workers by recording the number of keystrokes per minute, the precise time and location of any errors, the amount of time it takes to process each form or complete each task, and the length of any breaks (Hébert, 2002). Employers may monitor employees' use of telephones by programming computers to count the number and type of calls and call-backs, the number of messages opened and waiting, the number of seconds before the call is answered, the number of times a caller is put on hold, the precise duration of each call, and the time period between calls (Hébert, 2002). Computers can be programmed to monitor the number of drafts of computer documents and the number of revisions per line of dictation (Hébert, 2002).

Recent software developments have greatly expanded the ability of employers to monitor employees' computer network and Internet use (United States Government Accounting Office, 2002, p. 5). Software enables employers to secretly, and in real-time, monitor employees' use of networked computers including individual monitoring of each connected computer (Frayer, 2002). Software enables employers to capture the images from an employee's computer screen at random intervals and then compress those images to provide documentation of all computer work (Towns, 2002). Software also may reveal the online activities of all employees, including websites visited and the length of the employees' visits to websites (Hébert, 2002). Software also is available that allows employers to monitor employees' use of chat rooms, programs run, games played, files used, bytes transferred or downloaded, time spent downloading, and e-mail sent or received (Anderson, 2002; Net Threat Analyzer, 2002) Additionally, software may be used to monitor employees' computer hard-drives to identify pornography, music, or movies that have been downloaded in violation of copyright laws or workplace policies (Borland, 2002).

EMPLOYEE PRIVACY AND THE AT-WILL EMPLOYMENT RELATIONSHIP

Employment at-will is a doctrine that allows employers to discharge an employee for almost any reason or for no reason, as long as the discharge is not contrary to a statute or a contract (Cottone, 2002). Theoretically, the at-will doctrine is based on viewing the

relationship between employer and employee as a mutual relationship where either the employer or employee is free to terminate the relationship at any time (Cottone, 2002). However, the mutuality justification of the at-will rule has been much criticized because employees often have inferior bargaining power when compared to their employers (Cottone, 2002).

Some notable exceptions to employment at-will mitigate the harshness of the at-will doctrine. These exceptions to at-will employment limit the employer's ability to terminate at-will employees on the basis of a protected classification established under federal or state discrimination laws (Leonard, 1988). For example, it is unlawful under federal discrimination laws for an employer to treat employees differently with respect to terms and conditions of employment based on their sex, race, color, national origin, religion, age, or disability (Age Discrimination in Employment Act of 1967; Americans With Disabilities Act of 1990; Title VII of the Civil Rights Act of 1964). At-will employees are also protected from wrongful discharge for reasons that violate public policy, such as exercising a legal right to file a workers' compensation claim or serving on jury duty (*Frampton v. Central Indiana Gas Co*., 1973; *Garner v. Loomis Armored, Inc.*, 1996). Other exceptions to at-will employment protect employees covered by individual employment contracts or collective bargaining agreements that provide contractual rights greater than at-will employment, such as a right to be discharged only for just cause (Cottone, 2002; Leonard, 1988).

An understanding of workplace privacy for at-will employees begins with an understanding of privacy theory. "Privacy is the exclusive right to dispose of access to one's proper (private) domain" (Rothstein, 2000, p. 381). Electronic monitoring in the workplace is generally recognized to involve the legally recognized privacy tort claim categorized as "intrusion upon the plaintiff's seclusion, or into his private affairs" (Rothstein, 2000). The tort of invasion of privacy occurs when the defendant intentionally intrudes, physically or otherwise, upon the solitude or seclusion of the plaintiff in his private affairs or concerns, if a reasonable person would find the intrusion was highly offensive (*Fischer v. Mt. Olive Lutheran Church*, 2002).

Generally speaking, an at-will employee gives up his right to privacy in the workplace by agreeing to work for the employer:

> When a worker sells her capacity to labor, she alienates certain aspects of the person and puts them under the control of the employer. Thus in the U.S., workers in the workplace, except occasionally in restrooms and employee locker rooms, are not generally protected from surveillance on the grounds that the premises and equipment are possessions of the employer and the employee can have no legitimate expectation of intimacy or of protection from employer intrusion. The employee, in the employment-at-will setting, has implicitly consented to the employer's right to monitor the employee closely 'for any reason, no reason, or even reason morally wrong' or lose her job. [citations omitted] (Rothstein, 2000, p. 382)

The theory that at-will employees give up their rights to privacy when they enter the workplace underlies the failure of state tort laws to protect workplace privacy. Consequently, it is also true that employees who have brought tort claims of invasion of privacy related to electronic workplace monitoring have largely failed (Topolski & Palewicz, 2002). For example, courts that have considered privacy tort claims related to electronic monitoring of workplace e-mail systems generally fail to find that at-will employees have privacy rights that protect them from electronic monitoring in the workplace, or if privacy rights are found to exist, fail to find that employer monitoring of the workplace violates those rights (*McLaren v. Microsoft Corporation*, 1999; *Smyth v. Pillsbury Co.*, 1996). The ability of employers to adopt workplace policies reserving their rights to engage in electronic monitoring further

limits the privacy protections of at-will employees under state tort laws (*Garrity v. John Hancock Mutual Life Insurance Company*, 2002).

Unless an at-will employee has a statutory or contractual right to privacy, the employee has no privacy right that limits the employer's ability to engage in electronic monitoring of the workplace (Cottone, 2002). In contrast to at-will employees, employees who are covered by collective bargaining agreements may have contractual rights to privacy that arise from the collective bargaining agreement, and the collective bargaining agreement may also restrict an employer's right to terminate employees without just cause, notice, and procedural process (Cottone, 2002; National Labor Relations Act, 1935). Also in contrast to at-will employees, public employees may have rights to privacy and protections from arbitrary termination that are based on civil service legislation and state or federal constitutions (Cottone, 2002; *U.S. v. Simmons*, 2000). This paper examines the federal statutory provisions that confer a right to privacy on at-will employees in the private sector workplace with respect to electronic monitoring, including statutes that have been recently amended in response to the War on Terrorism.

FEDERAL PRIVACY STATUTES AND ELECTRONIC MONITORING BY EMPLOYERS

The basic federal protection for the privacy of electronic communications is found in the Electronic Communication Privacy Act (ECPA) of 1986, which encompasses federal wiretapping laws and federal laws prohibiting unauthorized access to communications in electronic storage (*Konop v. Hawaiian Airlines*, 2002).[2] Under these federal privacy statutes, it is unlawful for anyone, including an employer, to intentionally "intercept" the content of a wire, oral, or electronic communication (Title I violations) (ECPA, 1986). It is also a federal crime for anyone to "access" without "authorization" a facility providing electronic communication service and thereby obtain access to a wire or electronic communication while it is in electronic storage (Title II violations) (ECPA, 1986).[3]

Unless the interception or unauthorized access of a wire, oral, or electronic communication is covered by one of several statutory exceptions or authorized by government compulsion, such as a court order, violation of these statutes is a federal crime. Title I contains exceptions for "business use in the ordinary course of business," "providers of communication systems," and "consent" (Kesan, 2002). Title II contains exceptions for "providers of communications" and "authorization by users of communications systems" (Kesan, 2002). For a summary of key provisions of the ECPA, see Table I. The ECPA also gives private citizens, including employees, the right to sue for civil damages when there has been an unlawful interception or access to a communication in electronic storage in

[2]"In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, which was intended to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to 'address the interception of . . . electronic communications.' S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557. Title II of the ECPA created the Stored Communications Act (SCA), which was designed to 'address access to stored wire and electronic communications and transactional records.'" On October 26, 2001 The Wiretap Act and the SCA were amended by the USA PATRIOT Act

[3]Federal privacy statutes set a minimum privacy protection for electronic communications, including those of employees, but State privacy statutes may be more protective of electronic communications privacy rights (GAO Study). Examination of state privacy statutes is beyond the scope of this paper, however, the ECPA may provide defenses for employers that can be used to escape any additional restrictions on electronic monitoring that are imposed by state wiretapping laws (18 United States Code Service Sections 2520(d) and 2707[e]).

Table I. Electronic Communications Privacy Act—Exceptions and Government Authorization to Intercept or Access Electronic Communications

	Title I	Title II
Coverage of the statute	Prohibits interception of the contents of oral, wire, or electronic communications. Covers telephone, e-mail, Internet chat, and voice mail conversations. May be limited to interception of communications in transit.	Prohibits unauthorized access to and disclosure of the contents of stored wire and electronic communications. Covers e-mail, Internet chat, and voice mail. May be limited to access of communications prior to delivery to intended recipient.
Business use exception	By subscriber of electronic communication service to intercept communications in the ordinary course of business. In *Briggs v. American Air Filter Co.* (1980), no violation when employer listened to an employee's telephone call with a competitor to ascertain if disclosing confidential information.	Not applicable
Provider exception	Electronic communications service provider may intercept the contents of a communication in the ordinary course of business. In *Watkins v. L.M. Berry & Co.* (1983), court held employer must cease listening to employee's telephone call as soon as call is determined to be personal.	Electronic communications service provider may access, disclose contents. In *Bohach v. City of Reno* (1996), no violation when employer provided pager and accessed and retrieved stored text messages.
Consent exception	Interception of the contents of a communication is lawful with the consent of a party to the communication, unless the interception is for the purpose of committing a crime or tort. Consent may be obtained expressly or implied from a provider's monitoring policy including workplace electronic monitoring policies.	Access is lawful with authorization by a user of the electronic communications service to access or disclose stored contents of the user or intended for the user. Authorization may be obtained expressly or implied from a provider's monitoring policy.
Government authorization exception	Government may authorize the employer to disclose, intercept the contents of a communications with a warrant, a court order, or a written government certification in certain emergency situations before an order can be obtained.	Government may authorize the employer to access or disclose the contents of a communication with a warrant or a subpoena.
Government requirement to retain a backup copy	By subpoena or court order may require an electronic communications service provider to retain a backup copy of the contents of a communication.	By subpoena or court order may require an electronic communication service provider to retain a backup copy of the contents of a communication.

violation of the privacy rights set out in these statutes. For a summary of criminal and civil liability under the ECPA, see Table II.

The ECPA has been ineffective as a tool to regulate employer monitoring in the workplace: "Once an employer meets an exception, the ECPA places no restrictions on the

Table II. ECPA Civil and Criminal Liability and Defenses Applicable to Employers

	Title I	Title II
Civil liability	One who intentionally violates the prohibitions may be sued for civil damages, punitive damages, attorneys' fees, and litigation costs.	One who knowingly violates this statute may be sued for civil damages (and punitive damages if the violation is willful or intentional), attorneys' fees and litigation costs.
	Damages include the greater of actual damages plus any profits made, or statutory damages from $100 a day for each day of violation up to $10,000.	Damages include actual damages plus any profits made but no less than $1000.
Criminal liability	Fines or imprisonment, or both; imprisonment may not exceed 5 years.	Fines and imprisonment, or both; imprisonment from 6 months to 2 years.
Good faith defenses to civil and criminal liability	Good faith reliance on a court warrant or order, grand jury subpoena, legislative authorization, or a statutory authorization.	Good faith reliance on a court warrant or order, grand jury subpoena, legislative authorization, or a statutory authorization.
	Good faith reliance on the request of an investigative or law enforcement officer to intercept communications in specified emergency situations before an order authorizing such interception can be obtained.	Good faith reliance on a government request to preserve records and other evidence pending receipt of a court order or other process.
Statute of limitations	Two years from discovery or first opportunity to discover violation.	Two years from discovery or first opportunity to discover violation.

manner and extent of monitoring, nor does it require that an employer notify employees of monitoring" (Kesan, 2002, p. 298). Several commentators have concluded that in view of the breadth of the exceptions under the ECPA, it will be difficult for employees to sue their employers under the ECPA for electronic monitoring in the workplace if the employers adopt comprehensive electronic communications policies (Kesan, 2002).

Recent Cases Find Workplace Monitoring Violates Federal Privacy Statutes

Two recent cases illustrate the workplace privacy protections for employees provided by the ECPA. Although these privacy protections are limited, employees prevailed in both of these cases. First, in *Fischer v. Mt. Olive Lutheran Church*, a youth minister, Fischer, was terminated and sued his employer, the Mt. Olive Lutheran Church, claiming the church violated Title I of the ECPA by eavesdropping on his personal telephone conversations at work (*Fischer v. Mt. Olive Lutheran Church*, 2002). A church manager listened to a telephone conversation between Fischer and an outside caller using a cordless telephone that tied into the employer's telephone system. Fischer allegedly discussed explicit sexual material that was homosexual in nature. The court evaluated the application of the ECPA's exception for "business use" to Fischer's Title I claim. This exception allows the employer to intercept the plaintiff's telephone conversation as long as the interception is in the "ordinary course of its business." The court refused to dismiss Fischer's Title I claim because it concluded the interception of Fisher's telephone conversation was not in the ordinary course of business. The

court found that Fischer's conversation was not a business call and monitoring a personal call under these circumstances was not justified by valid business concerns. The court questioned how a private telephone conversation raised safety concerns for church personnel that could justify monitoring an otherwise personal call, however sexually graphic and homosexual in nature it may have been. The court also reasoned that the church might have a legal interest in continuing to listen to the conversation if Fischer was speaking to a minor due to his job responsibilities as a youth minister. However it was undisputed that the employer's managers believed that Fischer was speaking with another adult. The court held that under Title I, the employer was required to cease listening to Fischer's telephone call as soon as it determined that it was personal and that Fischer was not speaking to a minor. The employer did not have a workplace policy permitting interception of employee telephone calls and other electronic communications, so the court did not apply the "consent" exception.

Fischer v. Mt. Olive Lutheran Church also clarifies that an employer's use of electronic monitoring to monitor employees' communications *outside the workplace* may violate Title II of the ECPA. A computer expert hired by the church used the church's computers to access Fischer's Hotmail account after a church manager guessed Fisher's password. The computer expert printed out the e-mail messages that he found in Fischer's e-mail account, including e-mail messages that appeared to be from a homosexual lover. The *Fischer* court ruled that the employer's access of an employee's off-site e-mail account that was not provided by the employer would violate Title II of the ECPA and the case should proceed to trial.

In the second case, *Konop v. Hawaiian Airlines* (2002), the 9th Circuit Court of Appeals remanded an employee's Title II claim for trial in a case that involved company managers accessing the employee's nonpublic and off-site website without authorization. Konop, a pilot for Hawaiian Airlines, created and maintained a website where he posted bulletins critical of the employer and the incumbent union and encouraged Hawaiian employees to consider alternative union representation. Konop created a list of people who were authorized to access his website, mostly pilots and other employees of Hawaiian Airlines, and denied other persons access to his site through access restrictions that required visitors to log on with a user name and password. Hawaiian Airlines argued that two employees who were authorized to access Konop's website had authorized a manager to access Konop's website using their names consistent with the Title II exception that allows persons who are users of an electronic communication service to authorize a third party to access the electronic communications intended for the user. The 9th Circuit held that because the two employees had not accessed Konop's website before they authorized Hawaiian Airlines manager to do so using their names, they were not "users" who could authorize management to access Konop's site. So as in *Fischer*, the employee prevailed on his privacy claims under the ECPA.

Federal Court Cases Narrow the Scope of Federal Privacy Statutes

Recent federal circuit and district court cases have interpreted the scope of the ECPA narrowly, effectively expanding both the ability of employers to monitor the workplace and the ability of government to engage in electronic monitoring for law enforcement and foreign intelligence surveillance. First, Title I of the ECPA has been interpreted to prohibit only interceptions of electronic communications *while they are in transit*. *Konop v. Hawaiian Airlines* (2002) held that an "interception" of an electronic communication is prohibited under federal law only when it occurs contemporaneously with the transmission

of the communication.[4] The 9th Circuit Court of Appeals held Konop's Title I claims were properly dismissed by the lower court because even if Hawaiian Airlines' accessed Konop's private secured website without authorization, Hawaiian Airlines did not intercept any electronic communications while they were in transit to or from Konop's website. The *Konop* decision is consistent with the 5th Circuit Court of Appeals decision in *Steve Jackson Games, Inc. v. U.S. Secret Service* (1994). In *Steve Jackson Games* the court held the employer did not unlawfully intercept electronic communications when it seized a computer containing unread e-mail messages because the seizure of the computer containing the unread e-mail messages occurred sometime after the transmission of the e-mail messages to the computer.

Courts have also narrowed the application of Title II of the ECPA. Title II violations of ECPA involve unauthorized access to stored electronic communications. Recent court cases have held that unauthorized access to stored electronic communications is only prohibited by federal law when the electronic communication is in *temporary storage prior to delivery to the intended recipient*. Title II is not violated when there is unauthorized access to electronic communications in storage after the communication has been delivered to the intended recipient and then stored. For example, in *Fraser v. Nationwide Mutual Insurance Company* (2001), Fraser, an insurance agent, sued Nationwide for wrongfully discharging him as an independent contractor. Fraser claimed Nationwide violated both Title I and Title II of the ECPA. Nationwide obtained Fraser's and another Nationwide agent's e-mail messages from storage on Nationwide's electronic file server and opened the messages, discovering an e-mail criticizing Nationwide's business practices that had been sent by Fraser and his fellow agent to one of Nationwide's competitors. The e-mail Nationwide retrieved from its storage site was in "posttransmission storage" because it had already been sent by Fraser and received by the intended recipient, so there was no Title II violation. The district court also held Nationwide's e-mail monitoring did not violate Title I because Title I only prohibits interception of private communications during the course of transmission, not after the communication has been received and stored. Here Nationwide obtained the e-mail communications after transmission.

In sum, when the employer provides the workplace electronic communiciations system, the ECPA does not prohibit an employer from electronically monitoring employee electronic communications (including e-mail, voice mail, or web communications), so long as the employer does not intercept those messages while they are in transit or retrieve them from temporary storage or backup storage before the intended recipient has retrieved the messages. Some electronic monitoring software allows employers to intercept employees' electronic communications in real-time and to access electronic messages that have not yet been read by the intended recipients (Frayer, 2002). Employers who engage in real-time monitoring or access unread electronic messages, and who do not have an electronic communications policy that adequately reserves the employers' right to monitor electronic

[4]However, the *Konop* case is important because it illustrates that federal labor laws may protect employee privacy from electronic monitoring when the employee communications take place outside the workplace and the employer's e-mail and other computer systems are not used. *Konop* held electronic monitoring by employers of secure websites created by employees and used to discuss and criticize company management and the incumbent union interferes with the employee's right to engage in protected concerted activity under the Railway Labor Act (RLA) of 1926, which covers air and rail employees (*Konop v. Hawaiian Airlines*, 2002). *E*mployees in private sector workplaces not covered by the RLA have analogous rights under Section 7 of the National Labor Relations Act (NLRA) of 1935. Section 7 of the NLRA protects employees in nonunion workplaces as well as those who are represented by a union (*Epilepsy Foundation of Northeast Ohio*, 2001).

communications, or have not otherwise obtained "consent" of persons being monitored, are at risk of violating the requirements of the ECPA. See Table II for a summary of civil and criminal liability provisions of the ECPA.

THE IMPACT ON WORKPLACE PRIVACY FROM THE USA PATRIOT ACT

In October, 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) amended provisions of the ECPA that prohibit interception of oral, wire, and electronic communications (Title I) and restrict access to stored wire and electronic communications (Title II). The USA PATRIOT Act has approximately 1000 sections, is over 340 pages in length, and is designed to respond to the events of September 11, 2001. The USA PATRIOT Act gives enhanced surveillance powers to the government that may affect every employer and provider of Internet communications. The Act also has the potential to significantly impact the privacy of employees in the workplace as employers and Internet Service Providers are recruited into the government's effort to protect national security. Some provisions of the USA PATRIOT Act are subject to "sunset" limitations that make them expire on December 31, 2005 if not renewed by Congress (Sunset provision) (USA PATRIOT Act, Section 224).

As a result of the USA PATRIOT Act's amendments to these federal laws, employers will likely be asked, and in some cases compelled, to provide private information about employees and former employees to law enforcement and other government agencies (Cinquegrana & Harper, 2002). The employers' new legal obligations include the possibility of employers receiving search warrants, court wiretap orders, pen–register and trap and trace orders, and subpoenas ("government orders")[5] or government requests to produce information about a former or current employee in conjunction with a criminal investigation or a government intelligence surveillance of potential terrorism activities. These new employer legal obligations are essentially obligations to engage in electronic monitoring and have workplace privacy implications. The discussion of these privacy implications of the USA PATRIOT Act for employers and employees are organized into two sections: (1) privacy implications of employer electronic monitoring obligations related to criminal investigations, and (2) privacy implications of employer electronic monitoring obligations related to foreign intelligence surveillance related to the War on Terror.

Privacy Implications of Employers' Electronic Monitoring Activities Related to Criminal Investigations

Two key sections of the USA PATRIOT Act have workplace privacy implications because they involve the employer's electronic monitoring of the workplace to assist law enforcement conducting criminal investigations.

[5]Generally these types of government orders require advance authorization by a judge. However, U.S. Attorney General is authorized to issue administrative surveillance orders in some circumstances, for example under statutes authorizing emergency interceptions of electronic communications without advance approval by a court and for short periods of time (18 U.S.C.S. § 2518[7]).

Employer Monitors E-mail and Voice Mail Communications for Government

First, under Section 209 of the USA PATRIOT Act, employers may be required to comply with search warrants, including search warrants for e-mail or voice mail messages of employees.[6] Prior to the USA PATRIOT Act, a search warrant was sufficient to obtain stored e-mail messages, but a court wiretap order was needed for the government to obtain stored voice mail messages. A court wiretap order is more difficult for the government to obtain and more protective of the privacy of those monitored. The USA PATRIOT Act allows government investigators to use a search warrant to obtain stored voice mail evidence related to an investigation of any criminal offense.

Employer Assists Government in Secret Electronic Searches of the Workplace

Second, an employer may be called upon to assist the government in secret searches of the workplace under "delayed notification" rules. Section 213 of the USA PATRIOT Act permits searches and seizures by the government without prompt notice to the subject of the search and seizure when the government is seeking evidence of a criminal offense. Section 213 searches and seizures have been characterized as "sneak and peek" because they authorize surreptitious searches and seizures (147 Cong. Rec., 2001). Prior to the USA PATRIOT Act, "sneak and peek" searches and seizures had only been permitted in two jurisdictions under court rulings by the 2nd and 9th Circuit Courts of Appeals (*U.S. v. Freitas*, 1986; *U.S. v. Villegas*, 1990). Now "sneak and peek" searches and seizures are lawful across the nation (147 Cong. Rec., 2001). Applying Section 213 to the workplace, employers may be required to secretly monitor an employee's electronic communications as part of a government search and seizure and be prohibited from disclosing its action to the employee under investigation.

Under Section 213, there are some limits on "sneak and peek" searches and seizures that balance the interests of law enforcement with the privacy interests of persons under surveillance. In order for the government's search and seizure to qualify for delayed notification of a search, the government must (1) demonstrate reasonable cause to believe that providing immediate notice would have an adverse result on the investigation; (2) make a showing of reasonable necessity to seize any tangible property, wire or electronic communication, or stored wire or electronic communication; and (3) provide for notice of the search and seizure within a reasonable time of the search and seizure (147 Cong. Rec., 2001). If a court approves an extension of the period of delayed notice, the time between the search and seizure and the notice can be lengthy.

When a government search and seizure includes delayed notification, it may require the provider of an electronic communication service to keep its participation in the search and seizure secret (ECPA, 18 U.S.C.S. § 2705[b]). For example, assume an employer provides e-mail or voice mail systems for the use of its employees and therefore is a provider of an electronic communication service. A court may order the employer to access stored e-mail and voice mail messages, provide them to law enforcement, and not to tell the employee under surveillance that these things have occurred. Ultimately, once the delayed notification period has expired, the government will be required to notify the employee of the search and seizure of the employee's e-mail or voice mail messages.

[6]Section 209 of the USA PATRIOT Act will expire December 31, 2005, under the Sunset provision.

Privacy Implications of Employers' Electronic Monitoring Obligations Related to Government Surveillance of Terrorism Activities

Several sections of the USA PATRIOT Act expand the ways that employers may become involved in foreign intelligence surveillance conducted by the government that relates to the War on Terrorism and impacts privacy expectations that relate to employees' electronic communications in the workplace. The involvement of employers in federal government foreign surveillance efforts occurs by virtue of the USA PATRIOT Act's amendments to the Foreign Intelligence Surveillance Act (FISA) of 1978. These amendments to FISA expand the federal government's authority to engage in foreign intelligence surveillance through electronic or physical searches and seizures in order to prevent international terrorism, including terrorist acts that may occur in the U.S. (FISA, 50 U.S.C.S. § 1804; FISA, 50 U.S.C.S. § 1823). The USA PATRIOT Act expands the concept of foreign intelligence surveillance to encompass surveillance of U.S. citizens and businesses and may involve employers in this effort.[7]

Pen Register and Trap and Trace Devices Maybe Used to Monitor Workplace Electronic Communications

Under Section 214 of the USA PATRIOT Act, the Federal Bureau of Investigation (FBI) now has enhanced ability to use "pen register and trap and trace devices" when it is relevant to an investigation of international terrorism, clandestine intelligence activities, or foreign intelligence matters.[8] Pen register and trap and trace devices enable the FBI to trace communications in an electronic environment, such as recording phone numbers dialed from a particular telephone (147 Cong. Rec., 2001). Section 214 only authorizes the FBI to use pen register and trap and trace technology in a manner that does not capture the *contents* of wire or electronic communications. The use of a pen register and trap and trace device that does not capture the contents of a communication is not considered a search and seizure requiring a showing of probable cause (147 Cong. Rec., 2001). For example, a pen register and trap and trace device may now be used to trace communications made over the Internet including activity on a computer network or Internet Service Provider.

Section 214 permits the FBI to obtain an order for a pen register and trap and trace device to monitor the electronic communications of U.S. Persons. The term "U.S. Persons" includes U.S. citizens, permanent U.S. residents, and U.S. businesses (FISA, 50 U.S.C.S. § 1801[i]). Prior to the USA PATRIOT Act, in order to get authorization for pen register or trap or trace monitoring, federal investigators were required to show a court that the person targeted by a pen register or trap and trace device was in contact with an "agent of a

[7] Recently a federal appellate court held that Foreign Intelligence Surveillance Act (FISA) court orders authorizing electronic surveillance may authorize gathering information that may be used for prosecution of crimes unrelated to foreign intelligence surveillance as well as for foreign intelligence surveillance purposes (*In Re: Sealed Case*, 2002). Essentially the lower court had held there must be a well-defined wall separating domestic police agencies from spy agencies, but the appellate court held the USA PATRIOT Act made any such wall obsolete and unnecessary. The American Civil Liberties Union and other petitioners unsuccessfully filed a motion to intervene in the case in order to seek review of the decision by the U.S. Supreme Court (*American Civil Liberties Union v. U.S.*, 2003).

[8] Section 214 of the USA PATRIOT Act will expire December 31, 2005, under the Sunset provision.

foreign power" (147 Cong. Rec., 2001). Now, there is no requirement that the government show the person to be placed under surveillance had contact with an agent of a foreign power. An investigation targeting a U.S. citizen using a pen register and trap and trace device is lawful as long as the investigation is relevant to protect against: (1) international terrorism; (2) clandestine intelligence; or (3) foreign intelligence not concerning a U.S. citizen (147 Cong. Rec., 2001). An investigation of a U.S. citizen cannot be based solely on activities protected by the First Amendment to the U.S. Constitution (147 Cong. Rec., 2001).

As a result of Section 214, businesses and their employees may have their wire and electronic communications monitored by pen register and trap and trace devices when the monitoring is relevant to international terrorism or one of the other covered purposes. In such an investigation the government is not required to show there is probable cause for the monitoring. However, because the FBI is not permitted to monitor a U.S. person's electronic communications using a pen register and trap and trace device for the sole reason that the person is exercising his or her first amendment rights, government monitoring using pen register and trap and trace devices would not be permitted simply because the person is a member of a local mosque or peacefully protested the U.S. military's involvement in Afghanistan or Iraq.

Employers Obligations to Provide Electronic Records for Government Intelligence Surveillance Efforts

Section 215 of the USA PATRIOT Act also amends FISA and involves employers in the federal government's international terrorism and foreign intelligence surveillance efforts. Under Section 215, employers and other persons may be asked or ordered to provide access to business records and other "tangible" items to the FBI under FISA.[9] The purpose of Section 215 is to enhance the FBI's ability to gather information related to investigations of (1) international terrorism, (2) clandestine intelligence activities, and (3) foreign intelligence surveillance not concerning U.S. citizens. Consistent with the expansion of the government's ability to obtain orders for pen registers, etc., the business records the FBI may obtain in an investigation of international terrorism or clandestine intelligence activities may relate to "U.S. persons," including employees and former employees that are U.S. citizens, and are no longer restricted to records concerning "agents of foreign powers" (147 Cong. Rec., 2001).

Section 215 enables the FBI to get an order requiring the provider of business records to keep its production of records *secret*. Under such a "gag" order, the provider of business records may not disclose the FBI's effort to obtain business records. An employer who is required to provide the FBI access to its business records may only disclose that it is required by government order to produce business records to persons who need to know about the order in order to comply with it, and this does not include the person under surveillance.

Because the access to business records provided by Section 215 seem to require only the production of business records that are "tangible things," it is not clear whether Section 215 allows the FBI to obtain production of electronic records in storage or to require the

[9] Section 215 of the USA PATRIOT Act will expire December 31, 2005, under the Sunset provision.

employer to intercept wire, oral, or electronic communications, for example, using real-time monitoring. However, FISA also authorizes the federal government to obtain a wiretap order requiring interception of foreign intelligence communications (FISA, 50 U.S.C.S. § 1804). When FISA is read in conjunction with other provisions of the ECPA, it is clear that employers may be required to produce or intercept electronic communications of their employees for foreign intelligence surveillance purposes.[10] This is because the ECPA provides for assistance by providers of electronic communication services (including employers) and their employees, agents, and other persons to the FBI acting under a FISA warrant or court order. The assistance may be in the form of provision of information, facilities, or technical assistance to persons who are authorized by law to intercept electronic communications or conduct electronic surveillance under FISA (28 U.S.C.S. § 2511(2)(a)[ii][FISA Assistance]).

Section 218 of the USA PATRIOT Act amends FISA to extend the federal government's powers to conduct electronic or physical surveillance when a *significant purpose* of the surveillance is to obtain foreign intelligence surveillance (50 U.S.C.S. § 1804(a)(7)[B]).[11] The effect of this change is to expand the FBI's electronic surveillance powers to cover wiretaps that collect evidence for regular domestic criminal cases, as long as a significant purpose of wiretap is foreign intelligence (*In Re: Sealed Case, U.S. Foreign Intelligence Court of Review*, 2002). Because of the expanded nature of information that the government is entitled to collect under FISA, and the ECPA's FISA Assistance rules requiring electronic communication providers to assist the government with information, facilities, or technical assistance, the employers' obligations to engage in electronic monitoring pursuant to government orders have likewise been expanded.

Under the ECPA, providers of wire or electronic communication services may be required to provide the information, facilities, or assistance to the FBI *secretly*—providers and their employees and agents may not disclose the existence of the interception or surveillance or the device used for this purpose unless required by legal process (ECPA, 18 U.S.C.S. Section 2511(2)(a)[ii]). Even when disclosure of the interception or surveillance is required by legal process, the person making the disclosure must first give notice to the government official who made the request (ECPA, 18 U.S.C.S. Section 2511(2)(a)(ii)[B]). A provider who fails to keep its assistance secret as required by the ECPA may be liable for civil damages (ECPA, 18 U.S.C.S. Section 2511(2)(a)[ii]). However, if an electronic communication provider supplies the information, facilities, or assistance required under government order and keeps its required assistance to the government secret as required by the ECPA, the provider and its employees and agents are immune from legal actions in any court (ECPA, 18 U.S.C.S. Section 2511(2)(a)[ii]). In sum, employers, who are electronic service providers and in good faith provide information, facilities, or assistance to a government official who has presented a FISA warrant or court order, are not liable for civil damages for violations

[10] Section 218 is one of several amendments to FISA that expand the scope of FISA wiretaps. For example, Section 201 of the USA PATRIOT Act amends the ECPA to authorize the government to intercept wire, oral or electronic evidence under a wiretap order for federal offenses that are specifically tailored to terrorist threats (147 Cong. Rec., 2001). And Section 202 of the USA PATRIOT Act amends the ECPA to authorize the government to get a wiretap order to respond to crimes of computer fraud and abuse that are committed by terrorists to support and advance their illegal objectives (147 Cong. Rec., 2001).

[11] Section 218 of the USA PATRIOT Act will expire December 31, 2005, under the Sunset provision.

of the ECPA, and may not be sued in any court for providing the information, facilities, or assistance.

USA PATRIOT Act Expands Employers' Rights to Electronically Monitor the Workplace

The USA PATRIOT Act also creates some new employer rights that relate to electronic monitoring of the workplace. The most important new right arises from Section 217 of the USA PATRIOT Act, which creates a new "computer trespasser" exception to the ECPA.[12] This exception authorizes law enforcement to assist employers who are providers of electronic communications systems when hackers or other unauthorized persons have accessed the employers' computer systems. Before the USA PATRIOT ACT, law enforcement agencies needed a search warrant to intercept the contents of Internet communications sent by a computer trespasser (for example, a computer hacker), even if the owner of the computer system under attack gave its consent for law enforcement to intercept electronic communications on that system. Delays in obtaining a warrant often impaired law enforcement efforts to apprehend the hacker. Now, employers can permit law enforcement to intercept communications on the employers' computer systems.

However, the computer trespasser exception does not permit the employer to authorize law enforcement to obtain any communications other than those from the computer trespasser, so precision in interception is still required. Technology to intercept only the desired communications is not always available today. Overbroad monitoring may violate federal and state privacy rights when the monitoring exceeds the scope of the computer trespasser exception. The computer trespasser exception does not permit an employer to authorize monitoring of current employees who are authorized to access the employer's computer systems. This is because Section 217's definition of computer trespassers excludes persons who are "authorized" to access a protected computer and persons who have an "existing contractual relationship" with the owner or operator of the computer when the contractual relationship includes authorization to access the computer. Former employees seem to fall within the definition of computer trespasser as long as they are no longer authorized to access the employer's computer systems.

Employers who are required or authorized to conduct electronic monitoring under the ECPA may benefit from the ECPA's "good faith reliance" defense that is found in both Title I and Title II (ECPA, 18 U.S.C.S. Sections 2520(d) and 2707[e]). The defense applies when the employer is required by the government to intercept communications or to produce stored electronic communications. The defense prohibits anyone from bringing a civil or criminal cause of action under the ECPA or any other law against a person who acts in good faith in reliance on a government request or order, including written certifications by government officials, search warrants, court wiretap, or pen register and trap and trace orders, or subpoenas. Although this defense is not new, Section 215 of the USA PATRIOT Act expands the defense to include production of business records and other things under an order pursuant to Section 215. The availability of the good faith reliance defense to shield employer electronic monitoring activities makes it even more

[12] Section 217 of the USA PATRIOT Act will expire December 31, 2005, under the Sunset provision.

difficult for employees to challenge electronic monitoring in the workplace as invasions of privacy.

USA PATRIOT Act Creates Civil Liability for the U.S. Government for Unauthorized Disclosure of Electronic Communications

Section 223 of the USA PATRIOT Act creates new civil liability for unauthorized disclosures of electronic communications by investigative, law enforcement, or government officers.[13] Section 223 also defines authorized disclosures, clarifying situations where disclosure of information by investigative, law enforcement, or government officers is permitted. Where disclosure is not authorized by Section 223, and communications obtained by pen register and trap and trace devices, wiretaps, and search warrants are unlawfully disclosed by the government, courts may find the U.S. government civilly liable and award damages to injured parties. Damages recoverable include the greater of actual damages or $10,000 plus reasonable litigation costs. Section 223 also provides for administrative discipline of federal officers or employees who willfully or intentionally violate the new restrictions on unauthorized disclosure of electronic communications. Section 223 is an important new mechanism to protect the reputations and privacy interests of employees and employers in light of the expanded government surveillance tools provided in the USA PATRIOT Act.

PRIVACY CONCERNS ABOUT ELECTRONIC MONITORING SHARED BY EMPLOYERS AND EMPLOYEES

The combined actions of Congress and the courts have effectively expanded the ability of employers to monitor electronic communications of employees without violating federal privacy laws. But there are negative implications for the privacy of employers and employees alike that arise from these recent developments. For example, the enhanced ability of the government to compel businesses to monitor their electronic communications systems for law enforcement or foreign intelligence surveillance purposes decreases the sphere of privacy of electronic communications of both employers and employees. These decreased privacy expectations arise from the fact that employers and employees alike may be the subject of electronic monitoring by the government or electronic monitoring on the government's behalf. An employer's vendor or customer could be required by the government to secretly monitor activities of an employer or its employees, for example.

The USA PATRIOT Act also expanded the ways that electronic communication providers *that serve the public* (including Internet Service Providers) may access and disclose stored electronic communications of those who use their services. Employers and employees alike may use the services of Internet Service Providers (ISPs) and share privacy concerns about reduced privacy expectations in electronic communications made using ISPs. Under certain circumstances ISPs are permitted to access and/or disclose the contents of electronic communications made by employers and employees on their services to law enforcement and to other persons. Currently, the ECPA allows ISPs to access or disclose the contents of communications in electronic storage on their services (1) to an addressee or intended recipient of the communication; (2) with the lawful consent of the originator

[13]Section 223 of the USA PATRIOT Act will expire December 31, 2005, under the Sunset provision.

or an addressee or intended recipient of such communication; and (3) under a business use exception when it is necessary to provide the service or protect the provider's rights or property.

The USA PATRIOT Act expanded the permitted disclosures of communications by ISPs to law enforcement. Section 212 of the USA PATRIOT Act amended the ECPA to permit electronic communication services that serve the public to disclose the contents of communications in order to protect life and limb.[14] Lawful disclosures of the contents of a communication to law enforcement now include (1) disclosures by a service provider who inadvertently obtains content of stored communication that appears to pertain to the commission of a crime, and (2) disclosures by a service provider who reasonably believes there is an emergency that involves immediate danger of death or serious injury to any person that requires disclosure of the information without delay.[15]

Under rules permitting disclosure of customer records, ISPs may also divulge a record or other information relating to a subscriber or a customer of its services. These customer record disclosure rules do not permit disclosure of the contents of a communication. The information that may be disclosed under this exception includes information about the subscriber or customer's account, such as the subscriber's name, address, billing records, and length of service. Section 212 of the USA PATRIOT Act expanded the customer record information that may be divulged by an ISP to include records of session times, network addresses, and source of payment, including credit card or bank account numbers. ISPs may disclose customer record information to a governmental entity when the provider reasonably believes that an emergency involving immediate danger of death or serious injury to any person justifies disclosure of the information.

Because both employers and employees may be subscribers and users of Internet Service Providers, both employers and employees have privacy concerns about the extent of permitted disclosures by ISPs. Under the ECPA's expanded access and disclosure rules for ISPs, business communications that are generally considered proprietary or confidential by employers may be accessed or disclosed by ISPs, a privacy concern for employers. An ISP also may access or disclose communications that employees consider private, including employees' communications made using employers' or employees' computer systems and communicated over ISPs. The decreased privacy expectations resulting from the USA PATRIOT Act amendments may discourage the use of the Internet and e-mail as an avenue of communications. Employers have one key privacy-related advantage because they are more likely to operate their own servers for Internet connections, thus avoiding the use of an ISP, and the privacy concerns of using ISPs.

NATIONAL SECURITY INTERESTS CAUSE TIP IN THE PRIVACY BALANCE IN THE WORKPLACE

Analysis of the privacy protections that relate to electronic monitoring of the workplace supports a conclusion that both employees and employers have reduced privacy protections

[14]Section 212 of the USA PATRIOT Act will expire December 31, 2005, under the Sunset provision.

[15]Privacy concerns related to ISPs' permitted disclosures to the government have been enhanced by provisions in the Homeland Security Act of 2002 (Firestone, 2002). Section 225 of the Homeland Security Act extends the good faith defenses under Title I and II of the ECPA to ISPs. Under Section 225, an ISP may make disclosures of the contents of electronic communications to federal, state, or local government entities when the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency (Homeland Security Act of 2002).

as a result of recent changes in U.S. law. However, the privacy impact is not equally born by employers and employees.

At the federal level, employees and employers have reduced privacy protections that are largely a result of laws passed in response to national security threats. Both employers and employees may complain that the USA PATRIOT Act reduces the expectations of privacy that each holds related to electronic communications in the workplace. The communications of the employer as well as the employee may be the subject of electronic monitoring instigated by the government in pursuit of law enforcement or foreign intelligence surveillance objectives. Employers and employees may both be the subject of secret electronic monitoring under government orders that relate to the War on Terrorism or other criminal investigations. Employers and employees who communicate using ISP have reduced expectations of privacy in those communications as a result of the USA Patriot Act's amendments to the ECPA. This reduced privacy expectation may expose employers' trade secrets and other proprietary information in favor of enhanced ability of the government to obtain this information for law enforcement or foreign intelligence surveillance purposes. Likewise the ability of an ISP to access or disclose an employer's communications may be a serious concern for employers seeking to protect the privacy of their business affairs. In sum, both employers and employees share privacy concerns as a result of the recent changes in federal privacy laws.

However, employers and employees do not have equivalent privacy concerns with respect to electronic monitoring of electronic communications in the workplace. While employers and employees share reduced privacy expectations in their electronic communications with respect to government intrusions for national security purposes, employers still possess considerably more privacy rights than do employees in electronic communications related to the workplace. In fact, prior to the USA PATRIOT Act, employee privacy rights in their electronic communications in the workplace were nearly nonexistent as demonstrated by the failure of state tort law to provide protection and restrictive interpretations by the courts on the scope of the ECPA. And, as explained previously in this paper, employees' privacy rights have been further reduced by the USA PATRIOT Act's amendments to the ECPA.

On the other hand, employer privacy rights in electronic communications in the workplace were significant prior to the USA PATRIOT Act's amendments because many of those rights depended on the employer's status as the provider or owner of the electronic communications system used for workplace communications. Generally the employer, as the provider of its electronic communications systems, has and will continue to have significant privacy rights that protect its communications from intrusions by outsiders and give the employer the right to monitor employees' electronic communications on its systems. And the employer's ability to utilize its own servers for Internet communications also limits the impact of recent expansions of the rights of ISPs to make disclosures of communications and customer records to the government.

Significantly, at-will employees are further burdened by reduced privacy expectations in their electronic communications because of the relationship between employee privacy rights and at-will employment. Increased electronic monitoring of electronic communications in an at-will workplace, even under the compulsion of government national security interests, has further tipped the balance of power between employer and employee in favor of the employer. As government empowers or compels employers to monitor their electronic communications systems to further national security interests, information that could

compromise an employee's job security may come to the attention of an employer. Consider a situation in which an employer receives a court order to electronically monitor and produce the voice mail and e-mail communications of an employee who is Muslim or of Middle Eastern descent on behalf of the FBI, including instructions to keep the monitoring secret from the employee. Will the employer assume the employee under investigation is a terrorist or other criminal? Will the employer terminate the employee to remove a possible threat from the workplace, without evidence of wrongdoing? If the employer is barred from disclosing to the employee that the employer is under government compulsion to electronically monitor the employee's electronic communications, how will the employee be able to challenge the reasons that the employer may use for termination? These concerns are not trivial to at-will employees.

Although the balance of power in at-will employment may shift further in favor of employers as a result of the USA PATRIOT Act, employers should exercise this power with moderation. The current national security concern does not justify unnecessary workplace monitoring or arbitrary dismissals of employees based on inconclusive evidence obtained through electronic monitoring. There are two important reasons for this conclusion.

First, except when compelled by the government to respond to a government order to monitor, employers should exercise restraint in electronic monitoring of the workplace and termination decisions based on evidence obtained through electronic monitoring. This restraint is justified because it is consistent with the text and purpose of the USA PATRIOT Act. Section 102 of the USA PATRIOT Act expressly condemns blaming Arab and Muslim Americans as a group for the violent acts of other persons who may be of the same national origin: "The concept of individual responsibility for wrongdoing is sacrosanct in American society, and applies equally to all religious, racial, and ethnic groups." Section 201 of the USA PATRIOT Act also expressly condemns national origin discrimination:

> It is the sense of Congress that—(1) the civil rights and civil liberties of all Americans, including Arab Americans, Muslim Americans, and Americans from South Asia, must be protected, and that every effort must be taken to preserve their safety; (2) any acts of violence or discrimination against any Americans be condemned; and (3) the Nation is called upon to recognize the patriotism of fellow citizens from all ethnic, racial, and religious backgrounds.

Second, employers should exercise restraint in electronic monitoring of the workplace and termination decisions because it makes good business sense to minimize the likelihood of discrimination claims and expensive litigation. At-will employees are protected by federal and state nondiscrimination laws that prohibit employment discrimination on the basis of race, national origin, and religion, among other protected classifications (Cottone, 2002; Title VII of the Civil Rights Act of 1964). An employee who is Muslim and of Middle Eastern descent could arguably claim protection under all three of these protected classifications. If the discrimination claimed is proven by the employee to be based on an employee's protected classification, the employee will have a remedy under state or federal discrimination laws that may include compensatory and punitive damages, attorneys' fees, and litigation costs (Title VII of the Civil Rights Act of 1964).

An at-will employee terminated from employment when the employer is aware that the employee is under surveillance by the government will have many hurdles to jump through in order to prove the termination was an act of unlawful discrimination. And because of the secrecy that often accompanies employer monitoring conducted to further government surveillance, the employee who is terminated may not even know whether he or she was under government surveillance that enlisted the employer's electronic monitoring

capability. However, even if the employee is ultimately unsuccessful in proving unlawful discrimination, the expense and difficulty of defending employment discrimination claims is a good reason for employers to exercise restraint in electronic monitoring activities and termination decisions based on information obtained through electronic monitoring.

CONCLUSION

In light of the War on Terror and the current state of workplace privacy law in this country, at-will employees have precious few privacy protections from electronic monitoring in the workplace. Recent cases interpreting federal privacy statutes have effectively expanded the employer's ability to electronically monitor the workplace. And the recent expansion of the government's ability to electronically monitor communications in the War on Terrorism has only exacerbated workplace privacy concerns as they expand employer obligations to assist the government's electronic monitoring efforts. Consistent with the purpose and text of the USA PATRIOT Act's amendments to federal privacy laws covering electronic communications, and the risk of litigation concerning discrimination claims, employers should exercise restraint in the use of information obtained from electronic monitoring to discipline or discharge at-will employees. Although the employer may obtain information from electronic monitoring in its role to assist the government in surveillance or criminal investigations that it would not otherwise possess, mere suspicion of a terrorist in the workplace is hardly the type of information that reasonably supports a discharge and may well lead to discrimination claims.

ACKNOWLEDGMENTS

The author extends her gratitude to her husband, Brian J. King, Attorney, Schwabe Williamson & Wyatt, Portland, Oregon, who reviewed drafts of this paper.

REFERENCES

Age Discrimination in Employment Act of 1967, 29 U.S.C.S. § § 621 *et seq.* (1967).

American Civil Liberties Union, et al. v. United States (American Civil Liberties Union v. U.S.), 123, S.Ct 165(Mem), 155 L.Ed.Zd 309, 2003 WL 1447870 (2003).

American Management Survey (2001). Workplace monitoring & surveillance. Retrieved October 11, 2002, from http://www.amanet.org/research/archives.htm

Americans With Disabilities Act of 1990, 42 U.S.C.S. § § 12101 *et seq.* (1990).

Anderson, M. R. (2002). Identifying internet activity, computer forensics goes to cyber space. Retrieved April 4, 2003, from http://www.forensics-intl.com/artipfl.html

Bohach v. City of Reno, 932 F. Supp 1232 (D. Nev. 1996).

Borland, J. (2002). Employers crack down on workplace downloads, *ZDNet News*. Retrieved April 4, 2003, from http://zdnet.com.com/2100-1105-961262.html

Briggs v. American Air Filter Co., 630 F.2d 414 (5th Cir. 1980).

Cinquegrana, R. J., & Harper, R. M. (2002). The USA PATRIOT Act: Affects on American employers and businesses. *Boston Bar Journal*, *46*, 10–16.

Computer Forensics Defined (2002). *New Technologies, Inc.* Retrieved April 4, 2003, from http://www.forensics-intl.com/def4.html

Cottone, E. R. (2002). Employee protection from unjust discharge: A proposal for judicial reversal of the terminable-at-will doctrine. *Santa Clara Law Review*, *42*, 1259.

Electronic Communications Privacy Act (ECPA) of 1984, Pub. L. No. 99-508, 100 Stat. 1848 (Title I of the ECPA amended the Wiretap Act of 1968 and is codified at 18 U.S.C.S. § § 2510 *et seq.*; Title II of the ECPA created the Stored Communications Act and is codified at 18 U.S.C.S. § § 2701–2711).

Epilepsy Foundation of Northeast Ohio, 331 N.L.R.B. No. 92, 2000 WL 967066 (2000), *aff'd in part, rev'd in part*, 268 F.3d 1095 (D.C. Cir. 2001), *cert. denied*, 122 S. Ct. 2356 (June 10, 2002).

Evans, J. C. (2002). Hijacking civil liberties: The USA PATRIOT Act of 2001. *Loyola University of Chicago Law Journal*, *33*, 959–964.

Firestone, D. (2002, November 20). Senate Votes, 90-9, to set up homeland security department geared to fight terrorism. *The New York Times*, p. A1. Retrieved April 4, 2003, from http://www.nytimes.com

Fischer v. Mt. Olive Lutheran Church, 207 F. Supp.2d 914, 922, 928 (W.D. Wis. 2002).

Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C.S. § § 1801 *et seq.* (2002).

Frampton v. Central Indiana Gas Co., 260 Ind. 249, 297 N.E.2d 425 (1973).

Fraser v. Nationwide Mutual Insurance Company, 135 F. Supp.2d 623 (E.D. Pa. 2001).

Frayer, C. E. (2002). Employee privacy and internet monitoring: Balancing workers' rights and dignity with legitimate management interests. *Business Lawyer*, *47*, 858–859.

Garner v. Loomis Armored, Inc., 913 P.2d 377, 1996 Wash. LEXIS 109 (1996).

Garrity v. John Hancock Mut. Life. Ins. Co., 2002 WL 974676 at *1 (D. Mass. 2002).

Hébert, L. C. (2002). Methods and extent of employer use of electronic monitoring and surveillance. *Employee Privacy Law*, *1*, Section 8A:1.

Homeland Security Act of 2002, 6 U.S.C.S. § § 101 *et seq.* (2002).

In Re: Sealed Case No. 02-001 Consolidated With 02-002 – On Motions For Review of Orders of the United States Foreign Intelligence Surveillance Court (NOS. 02-662 AND 02-968) (*In Re: Sealed Case, U. S. Foreign Intelligence Surveillance Court of Review)*, 310 F3d 717, 2002 WL 31546991 (F.I.S.Ct. November 18, 2002).

Kane, B. P. (2001). 1984 in 2001: Monitoring employee e-mail usage. *Advocate (Idaho)*, *44*, 20.

Kesan, J. P. (2002). Cyber-working or cyber-shrinking?: A first principles examination of electronic privacy in the workplace. *Florida Law Review*, *54*, 296.

Konop v. Hawaiian Airlines, 302 F.3d 868, 870 (9th Cir. 2002) .

Leahy, M. C. M. (2002). Recovery and reconstruction of electronic mail as evidence. *American Jurisprudence Proof of Facts 41*, 1. (3d.)

Leonard, A. S. (1988). A new common law of employment termination. *North Carolina Law Review*, *66*, 631.

McLaren v. Microsoft Corporation, 1999 WL 339015 (Tex. App. 1999) (unpublished opinion).

National Labor Relations Act of 1935, 29 U.S.C.S. § 151–169 (2002).

Net Threat Analyzer (2002). *New Technologies, Inc.* Retrieved April 4, 2003, from http://www.forensics-intl.com/nta.html

Railway Labor Act of 1926, 45 U.S.C.S. § § 151–188 (2002).

Rogers, A. (2002). You got mail but your employer does too: Electronic communication and privacy in the 21st century workplace. *Journal of Technology Law and Policy*, *5*, 1.

Rothstein, L. E. (2000). Privacy or dignity: Electronic monitoring in the workplace. *New York Law Journal of International and Comparative Law*, *19*, 379.

Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).

Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C.S. § 2000d (2002).

Topolski, D. M., & Palewicz, A. W. (2002). Employee privacy rights in the electronic workplace. *Maryland Bar Journal*, *35*, 40–45.

Towns, D. M., (2002). Legal issues involved in monitoring employees' internet and e-mail usage. GigaLaw.com. Retrieved April 4, 2003, from http://www.gigalaw.com/articles/2002/towns-2002-01.html

United States Government Accounting Office (2002). Employee privacy, computer-use monitoring practices and policies of selected companies. *Report to the Ranking Minority Member, Subcommittee on* 21st *Century Competitiveness, Committee on Education and the Workforce, House of Representatives*. Retrieved April 4, 2003, from http://www.gao.gov/new.items/d02717.pdf

U. S. v. Freitas, 800 F.2d 1451 (9th Cir. 1986).

U.S. v. Simmons, 206 F.3d 392 (4th Cir. 2000).

U. S. v. Villegas, 899 F.2d 1324 (2d Cir. 1990).

USA Patriot Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (October 26, 2001).

Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th cir. 1983).

147 Cong. Rec. S10990 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy; The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, H.R. 3162, Section-by-Section Analysis).