

# **THE EAVESDROPPING EMPLOYER: A TWENTY-FIRST CENTURY FRAMEWORK FOR EMPLOYEE MONITORING**

Corey A. Ciocchetti<sup>†</sup>

---

<sup>†</sup> Assistant Professor of Business Ethics and Legal Studies, Daniels College of Business, University of Denver, J.D. Duke University School of Law, M.A. (Religious Studies) University of Denver. Please feel free to contact Professor Ciocchetti with questions or comments at [cciocche@du.edu](mailto:cciocche@du.edu). Thanks to the Daniels College of Business for the generous scholarship grant and course release awarded to support the creation of this article.

# **THE EAVESDROPPING EMPLOYER: A TWENTY-FIRST CENTURY FRAMEWORK FOR EMPLOYEE MONITORING**

## **ABSTRACT**

The twenty-first century continues to usher in new and increasingly-powerful technology. This technology is both a blessing and a curse in the employment arena. Sophisticated monitoring software and hardware allow businesses to conduct basic business transactions, avoid liability, conduct investigations and, ultimately, achieve success in a competitive global environment. Employees can also benefit when monitoring provides immediate feedback, keeps the workforce efficient and focused and discourages unethical/illegal behavior. The same technology, however, allows employers to monitor every detail of their employees' actions, communications and whereabouts both inside and outside the workplace. As more and more employers conduct some form of monitoring, the practice will shortly become ubiquitous. This trend is problematic because excessive and unreasonable monitoring can: (1) invade an employee's reasonable expectation of privacy, (2) lead employees to sneak around to conduct personal activities on work time, (3) lower morale, (4) cause employees to complain and, potentially, quit and (5) cause employees to fear using equipment even for benign work purposes.

The American legal system's effort to protect employee privacy is a patchwork of federal and state laws combined with the common law tort of intrusion upon seclusion. This regime is not properly equipped to defend against excessive invasions of privacy that come from increasingly-sophisticated monitoring practices. This article analyzes the problems with the current monitoring regime, evaluates the top contemporary monitoring techniques and proposes a framework around which Congress can craft new and more effective legislation dealing with employee monitoring. This framework classifies the top contemporary monitoring practices into four categories designed to balance employee privacy with enterprise protection - protection that occurs in the form of completing business transactions, protecting the company from liability and conducting or assisting in internal and external investigations. The categories form a sliding scale able to dictate the minimum amount of monitoring necessary to achieve the enterprise protection sought by management without excessively invading employee privacy.

# TABLE OF CONTENTS

INTRODUCTION	5
EMPLOYEE MONITORING IN THE UNITED STATES: THE CURRENT REGIME	8
TOP EMPLOYEE MONITORING PRACTICES	18
A. Access Panels	19
B. Attendance and Time Monitoring	21
C. Automatic Screen Warnings	22
D. Desktop Monitoring Programs	23
E. E-mail monitoring	23
F. Filters & Firewalls Restricting Internet Access	25
G. GPS, RFID & SmartCards	25
H. Internet Use Audits (Internet Monitoring)	27
I. Keystroke Logging	29
J. Physical searches	30
K. Social-Network & Search Engine Monitoring	31
L. Telephone, Text Message & Voicemail Monitoring	32
M. Video Surveillance	33
A NEW & EFFECTIVE EMPLOYEE MONITORING FRAMEWORK	35
A. The Low-Hanging Fruit: The Law Must Require Notice of Monitoring Practices	37
B. Category One: Best Practices	39
Access Panels	40
Attendance & Time Monitoring	40
Automatic Screen Warnings	41

C. Category Two: Risky Practices	41
Filters & Firewalls	42
Internet & Clickstream Data Monitoring	43
Social Network & Search Engine Monitoring	45
D. Category Three: Borderline Practices	48
E-Mail & Text Message Monitoring	48
GPS & RFID Monitoring	50
Physical Searches	52
E. Category Four: Poor Practices	54
Desktop Monitoring & Keystroke Monitoring	55
Phone & Voicemail Monitoring	57
Video Surveillance	58
CONCLUSION	61

# I. INTRODUCTION

Employers and employees have a love-hate relationship with technology. Both love the benefits of sophisticated hardware and software in a competitive global marketplace. Employees hate that the same technology tethers them to the workplace and records their electronic footprint. Employers hate the potential for liability, distraction and lost productivity when employees monopolize workplace technology for personal reasons. This paper analyzes the hate part of the equation.

Today, incessant distractions litter workplaces and entice workers to stray from their duties.<sup>1</sup> Fifteen years ago, these types of distractions existed only in an employee's imagination. If you are not convinced, calculate your average attention span during a typical workday. When did you last check ESPN.com for breaking news on your favorite team? How often do you log-in and monitor recent damage to your retirement accounts? How many Facebook friend requests or personal e-mails did you field in the last few hours? How long into a typical workday does it take you to electronically pay a bill, text your buddy down the hall, or check the forecast? As enticing as these distractions can be, you can bet that if you discover any of this information while on the job, your employer will acquire it as well. In fact, there is no need to be surprised when your boss approaches you and says, "Sorry about the recent breakup," or "Why did you call in with the swine flu last Friday and then e-mail pictures of your weekend excursion to twenty of your friends?"

These examples are not far-fetched. In fact, the majority of employers monitor the electronic activities of their employees in some form or another.<sup>2</sup> Most of this monitoring is perfectly legal and even prudent in today's employment arena. While employee monitoring remains a contentious issue,<sup>3</sup> employers have good reasons for checking in on their employees' activities. Sexual or pornographic e-mails and Web pages, containing pictures or merely sexually explicit language, can form the basis for a harassment lawsuit.<sup>4</sup> Excessive personal use of company broadband capacity or e-mail accounts will lead to decreased productivity, storage shortages and slower network operations.<sup>5</sup> Failing to monitor is also

---

<sup>1</sup> See e.g., Burst Media, *Online Sites: Go Online to Find the "Online At Work" Audience*, Nov. 1, 2007, available at <http://www.burstmedia.com/research/archived.asp> [hereinafter *Online Sites*] (finding that over 25% of an employee's work time is spent online conducting personal tasks. 18 to 24 year-old employees are likely to spend over 34% of their work time online conducting personal tasks - the highest percentage among all age groups surveyed).

<sup>2</sup> See generally, *2007 Electronic Monitoring & Surveillance Survey*, AM. MGMT. ASS'N, at 4, Feb. 28, 2008, available at <http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf> [hereinafter *2007 AMA Survey*] (surveying employer monitoring practices in various areas such as the Internet, e-mail, computer usage, etc.).

<sup>3</sup> See e.g., Caslon Analytics, *Privacy Guide*, CASLON.COM, <http://www.caslon.com.au/privacyguide22.htm> (last visited June 26, 2009) (stating that surveillance "by public and private sector employers of the activities of their workforce is both traditional and increasingly contentious, as employees question surveillance that may be systematic, invisible and often non-consensual.").

<sup>4</sup> See e.g., *Blakey v. Cont'l Airlines*, 751 A.2d 538, 543-44 (N.J. 2000) (discussing the facts of a sexual harassment case filed by a female airline pilot claiming, among other things, that her co-workers posted sexually explicit comments about her on Continental Airline's online bulletin board).

<sup>5</sup> See e.g., Association of Local Government Auditors, *Monitoring Internet Usage*, GOVERNMENTAUDITORS.ORG, Spring 2010, available at [http://www.governmentauditors.org/index.php?option=com\\_content&view=article&catid=47:accounts&id=594:monitoring-internet-usage-spring-2010&Itemid=123](http://www.governmentauditors.org/index.php?option=com_content&view=article&catid=47:accounts&id=594:monitoring-internet-usage-spring-2010&Itemid=123) (last viewed on April 22, 2010) (reiterating that employee Internet use for personal reasons can cause "bandwidth and storage shortages [particularly] from per-to-peer file sharing and audio/video streaming.").

likely to allow rogue employees to steal trade secrets or send out confidential information in violation of various federal and state laws.<sup>6</sup> On the other hand, employee monitoring pierces the veil of an individual's privacy and can decrease morale.<sup>7</sup> Excessive monitoring will merely cause employees to sneak around instead of following the rules. E-mails will be sent over employees' personal Hotmail or Yahoo accounts instead of over the company software. Text messages and phone calls will be made on personal cell phones instead of company lines. Employees will check sports scores and stock markets from their personal PDA instead of over their work computer.

With this in mind, employers must walk a fine line between shielding the enterprise and protecting employee privacy. Workable monitoring regimes must allow employers to use technology to monitor employee activities for the following three purposes: (1) Business Purposes; (2) Liability-Avoidance

---

<sup>6</sup> See e.g., Jared A. Favole, *Ex-Bristol-Myers Employee Charged with Stealing Trade Secrets*, WALL ST. J., Feb. 3, 2010, available at <http://online.wsj.com/article/BT-CO-20100203-718698.html> (discussing accusations against a Bristol Myers' technical operations associate for allegedly stealing company trade secrets in order to form a competing company in India) and Elinor Mills, *Microsoft Suit Alleges Ex-Worker Stole Trade Secrets*, C-NET.COM, Jan. 3, 2009, available at [http://news.cnet.com/8301-10805\\_3-10153616-75.html](http://news.cnet.com/8301-10805_3-10153616-75.html) (stating that an ex-employee "allegedly downloaded confidential documents onto his company-issued laptop . . . and then allegedly used a file-wiping program and a 'defrag' utility designed to overwrite deleted files in order to hide the tracks.").

<sup>7</sup> See e.g., Mia Shopis, *Employee Monitoring: Is Big Brother a Bad Idea?*, SEARCHSECURITY.COM, Dec. 9, 2003, available at (quoting an expert in electronic monitoring who stated that employee "monitoring is a bad idea . . . when it's used for Big Brother and micromanagement purposes. Organizations would be better off not doing it if they're going to scrutinize their employees' every move. If it creates a morale problem (and it will if it's not handled properly) all of its value is diminished.").

Employee monitoring can have the following negative effects:

1. An employee may suffer loss of self-esteem if she interprets the monitoring to indicate a lack of trust in her.
2. Employees may also question the fairness of the monitoring: are the right variables being measured; are the wrong variables being measured; is the measurement accurate? Fairness is also suspect considering that women and minorities receive a disproportionate amount of monitoring, as they make up a large percentage of the clerical ranks.
3. Worse, monitoring may be abused by the employer to intimidate and punish employees rather than help them improve.
4. Abuse may also take the form of voyeurism, union-busting, ferreting out whistleblowers, and creating pretenses to fire members of protected employee groups.
5. The accumulation of the above effects "takes its toll on workers and companies in terms of stress, fatigue, apprehension, motivation, morale, and trust; this results in increased absenteeism, turnover, poorer management, and lower productivity, not to mention higher health-care costs." Thus, monitoring may spoil the workplace environment, and it can have a detrimental effect on productivity. Productivity is harmed by the mental and physical manifestations of stress: depression and anxiety, including "wrist, arm, shoulder, neck, and back problems." It is estimated that employee stress costs employers fifty to seventy-five billion dollars annually.
6. Monitoring can also encourage employees to act in a counterproductive manner in an attempt to "game" the system.
7. Some employees are concerned that electronic monitoring will allow employers to increase the pace of work, creating sweatshops, not unlike those before the advent of progressive labor laws.
8. Unconditional acceptance of electronic monitoring also threatens the future of privacy in the workplace.

Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 319-20 (April 2002) [hereinafter *Cyber Working*] (internal citations omitted).

Purposes and (3) Investigatory Purposes.<sup>8</sup> Business purposes describe monitoring that aids employers in conducting and completing business transactions. Liability-Avoidance purposes describe monitoring that aids employers in preventing civil lawsuits or criminal prosecutions. Finally, Investigatory purposes describe monitoring that aids employers conducting an internal investigation.

This paper proposes an employee monitoring framework that fairly balances employer and employee interests for each key monitoring purpose mentioned above. Part II begins the process with an analysis of the current mishmash of regulation in the United States surrounding employee monitoring. Part III evaluates the top contemporary employee monitoring practices. The goal is to describe the technology, and analyze its implementation in the workplace. Part IV addresses the disconnect between the powerful technology and the decades-old legal regime by analyzing the importance of each monitoring technique in relation to the three key monitoring purposes. The section ends with a framework that identifies which monitoring technique is appropriate for which monitoring purpose considering both its privacy invasiveness and enterprise protection. The goal is to classify each of the top monitoring practices into one of the following categories:

1. **BEST PRACTICES** - monitoring that offers high enterprise protection and minimally invades employee privacy; these practices are appropriate for Business Purposes, Liability-Avoidance Purposes and Investigatory Purposes;
2. **RISKY PRACTICES** - monitoring that offers rather low enterprise protection and minimally invades employee privacy; these practices are most appropriate for Liability-Avoidance Purposes and Investigatory Purposes;
3. **BORDERLINE PRACTICES** - monitoring that offers high enterprise protection and is also highly invasive; these practices are only appropriate for all three monitoring purposes in limited circumstances; and

---

<sup>8</sup> Employer reasons for monitoring are diverse and important:

1. Electronic monitoring allows employers to make significant gains in the areas of productivity, quality, and safety.
2. Monitoring enhances productivity by facilitating more efficient resource scheduling, more immediate feedback, and more meaningful evaluations.
3. Quality likewise is improved, and customers benefit from better service and lower prices.
4. Monitoring is key to some safety initiatives, and better safety means lower insurance premiums and workers' compensation pay-outs.
5. Payroll and equipment costs can also be reduced by monitoring employees for personal use of company equipment and for taking excessive breaks. It has been estimated that employees wasted 170 billion dollars of employer time in one year alone. Further savings may be realized by curbing theft and legal liability.
6. In one year, it is estimated that employees stole the equivalent of 370 billion dollars from their employers. Monitoring can be used to detect illegal or wrongful deeds so that the offenders may be punished. For example, the data flow in and out of a company can be watched to find employees transmitting sensitive data or hackers attempting to crack into the system.
7. E-mail within the workplace also can be monitored to detect electronic harassment.
8. Alternately, monitoring may be used proactively to minimize respondeat superior liability to detect a problem before it happens.
9. As a final incentive, the law sometimes requires employers to monitor employees.

*Cyber-Working*, *supra* note 7, at 318-19 (internal citations omitted).

4. **POOR PRACTICES** - monitoring that offers low enterprise protection and is highly invasive; these practices are only appropriate for Investigatory Purposes and only in limited circumstances.

This classification system is designed to help legislatures (preferably Congress in the interest of a standardized, national workplace privacy regime) identify where to draw the line when it comes to future regulation of workplace technology. It is also helpful to employers to understand where courts might draw the reasonable expectation of privacy line in cases involving new and increasingly-sophisticated monitoring technology. Part V concludes with a call for the enactment of a standardized and balanced employee monitoring regime.

## II. EMPLOYEE MONITORING IN THE UNITED STATES: THE CURRENT REGIME

It is legal and common for employers to monitor the actions and expressions of their employees.<sup>9</sup> Unfortunately, the American legal system has failed to: (1) keep up with today's powerful monitoring technology and (2) provide the necessary privacy protection to employees.<sup>10</sup> Neither the Fourth Amendment, with its prohibition of unlawful searches and seizures, nor the federal Privacy Act of 1974 apply to the private employment arena.<sup>11</sup> In fact, the United States legal system operates under a piecemeal approach to electronic monitoring in private workplaces.<sup>12</sup> The only real restrictions on employers occur in rare situations where employees possess a "reasonable expectation of privacy" in the

---

<sup>9</sup> For the sake of cohesiveness, this paper discusses only the monitoring practices of private employers. For an analysis of employee monitoring and the privacy of employee information in the public sector, see generally Justin Conforti: COMMENT: *Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the Ortega Test in Quon v. Arch Wireless*, 5 SETON HALL CIR. REV. 461, 472-91 (Spring 2009) [hereinafter *Somebody's Watching Me*]; Rachel Sweeney Green, COMMENT: *Privacy in the Government Workplace: Employees' Fourth Amendment and Statutory Rights to Privacy*, 35 CUMB. L. REV. 639, (2004/2005); James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 4-18 (Winter 2005); and Paul F. Gerhart, *Employee Privacy Rights in the United States*, 17 COMP. LAB. L. 175, 176-205 (Fall 1995).

<sup>10</sup> See e.g., *Somebody's Watching Me*, *supra* note 9, at 464 (reiterating that if "employers monitor communications on workplace technology and employees inadvertently divulge personal information, employees will often struggle to find any legal protection, as the American legal regime does not provide any generally applicable, affirmative protection for employee privacy.").

<sup>11</sup> See e.g., *Brahmana v. Lembo*, 2009 U.S. Dist. LEXIS 42800, \*5 (N.D. Cal. 2009) [hereinafter *Brahmana*] (citing *Burdeau v. McDowell*, 256 U.S. 465, 474-75 (1921) [hereinafter *Burdeau*] and *U.S. v. Jacobsen*, 466 U.S. 109, 118 (1984)). The Supreme Court has held that the "Fourth Amendment gives protection against unlawful searches and seizures and . . . its protection applies to governmental action. Its origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies." *Burdeau* at 474-75. In addition, the federal Privacy Act of 1974 restricts employer collection and handling of personal information but only applies to federal agencies. 5 U.S.C. § 552a(a)(1) (2006).

<sup>12</sup> "No comprehensive statutory scheme supplements the common law to provide protection for employees' privacy or even simply from employer monitoring. Instead, a variety of federal and state laws offer only targeted and limited protections." Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 Cornell J. L. & Pub. Pol'y 609, 621 (2009) [hereinafter *Industrial Justice*].

workplace or where employers are stupid enough to violate flimsy state laws, federal laws or the common law tort of intrusion upon seclusion.<sup>13</sup>

This employer favoritism is deliberate as courts and legislatures adhere to the general philosophy that: (1) workplaces exist for work purposes, (2) employers provide technology and pay wages in return for performance and (3) liability issues override the instinct to enhance employee privacy interests. This philosophy has merit and comprises the most rational and workable foundation for an employee monitoring regime. This is especially true under the doctrine of employment at will which is an implicit agreement between employers and employees that employees may be fired for any legal reason.<sup>14</sup> However, it is important that the law recognize the power of contemporary monitoring technology, the ever-increasing number of hours contemporary Americans spend at work and the impact of excessive and undisclosed monitoring on employee morale. Such recognition must lead to a rebalancing of current legal provisions to the realities of the twenty-first century workplace. This section identifies the major problems with the current employee monitoring regime (especially in relation to the powerful monitoring technology discussed in Part III), while Part IV proposes a rebalancing that enhances workplace privacy without excessively hindering the employers' previously mentioned interests.

The relevant federal laws in play are the Electronic Communications Privacy Act of 1986 (ECPA)<sup>15</sup> and the Computer Fraud and Abuse Act (CFAA).<sup>16</sup> The ECPA has two relevant titles - the Wiretap Act (Title I) which regulates the intentional interception, use or disclosure of wire, oral and electronic communications<sup>17</sup> and the Stored Communications Act (Title II) which governs electronic

---

<sup>13</sup> See *id.* at 465 (stating that “[M]oreover, because the Fourth Amendment only applies when the government acts, private-sector employees have [basically] no statutory federal protection. While the Electronic Communications Privacy Act of 1986 protects against various kinds of electronic surveillance and interception of communications by public and private actors . . . this regime presents several potentially insurmountable hurdles for any employee who alleges his employer intercepted private communications on workplace technology.”). See also Nancy J. King, *Electronic Monitoring To Promote National Security Impacts Workplace Privacy*, 15:3 EMP. RESP. RTS. J. 127, 130-31 (2003).

<sup>14</sup> See e.g., William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOKLYN L. REV. 91, 125-27 (Fall 2003) (stating that “[d]espite the dubious proposition that someone can do something for no reason at all, the now famous, or infamous, iteration of employment at will encapsulates the absolute power of employers to govern the workplace. Although employment at will expressly addresses employers' absolute right to terminate employees, it is about much more. One who has the power to terminate also has the power to do as she pleases with respect to all terms and conditions of employment. At its core, employment at will is about employer power and prerogative.”).

<sup>15</sup> 18 U.S.C. § 2510 et seq. (2006). See also, *Konop v. Hawaiian Airlines, Inc.* 302 F.3d 868, 874 (9th Cir. 2002) [hereinafter *Konop*] (reiterating that “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.’”).

<sup>16</sup> 18 U.S.C. §1030 et seq. (2006).

<sup>17</sup> The Wiretap Act is Title I of the ECPA. See 18 U.S.C. § 2511 (2006). The Wiretap Act states that any person who:

- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
- (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication . . .
- (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . .

shall be punished [as stated subsequently in the statute].

*Id.* at § 2510(1). The ECPA defines electronic communication as “any transfer of signs, signals, writing, images sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce.” *Id.* at § 2510(12) (2006).

communications already transmitted and currently in storage.<sup>18</sup> The ECPA was intended to extend privacy protection from wire communications such as telephone calls to electronic communications such as e-mails and text messages.<sup>19</sup> The problem is that contemporary technology has advanced tremendously since 1986 and the ECPA is not equipped to keep pace.<sup>20</sup>

More specifically, under the Wiretap Act, an interception has been defined as accessing information using an electronic device while it is being transmitted;<sup>21</sup> once electronic information is stored, however, the wiretap provisions do not apply.<sup>22</sup> This is a major distinction because the vast majority of electronic communications are only “in transmission” for mere seconds before arriving at their destination.<sup>23</sup> If the provisions of the Wiretap Act seem favorable to employers, its strong exceptions seal the deal. The Wiretap Act exceptions allow monitoring if: (1) one of the parties involved consents (the Consent

---

<sup>18</sup> The Stored Communications Act is Title II of the ECPA (SCA). See 18 U.S.C. § 2701 (2006). The SCA states that: Except as provided [below,] whoever:

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . .

shall be punished as provided in [this section].

*Id.* at § 2701(a)(1)-(2). The penalties for violations of the SCA include fines and imprisonment. *Id.* at § 2701(b)(1)-(2).

<sup>19</sup> See e.g., *Brahmana*, *supra* note 11, at \*5.

<sup>20</sup> The ECPA was enacted before the creation of the World Wide Web and thus could not anticipate that a significant amount of contemporary monitoring technology involves the Web. See *Konop*, *supra* note 15, at 874 (stating that “the difficulty [in deciding how the ECPA must apply to contemporary technology] is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like [this] secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.”). In fact, there is evidence that:

[T]he language of the [Wiretap Act] makes clear that Congress meant to give lesser protection to electronic communications than wire and oral communications. Moreover, at this juncture, much of the protection may have been eviscerated by the realities of modern technology. [In fact] . . . the language may be out of step with the technological realities of computer crimes.

*United States v. Ropp*, 347 F. Supp. 2d 831, 833 (C.D. Cal. 2004) (citing *United States v. Councilman*, 373 F.3d 197, 200 (1st Cir. 2004)).

<sup>21</sup> The ECPA defines interception as the “aural or or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). “Courts applying the ECPA have consistently held that a qualifying ‘intercept’ occurs only where the acquisition of the communication occurs contemporaneously with its transmission by the sender.” *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, 14 (E.D. Va. 2009) [hereinafter *Global Partners*]. See also *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107, 113 (3rd Cir. 2003) (holding that an intercept under the ECPA must occur contemporaneously with the transmission from the sender); *Konop*, *supra* note 15, at 878-78 (9th Cir. 2002) (same); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F. 3d 457, 461-62 (5th Cir. 1994) (same); and *Wesley College v. Pitts*, 974 F. Supp. 375, 387 (D. Del. 1997) (same).

<sup>22</sup> See e.g., *Brahmana*, *supra* note 11, at \*5-6 (reiterating that the Ninth Circuit has declared that gaining access to stored communications does not violate the ECPA). This is an important distinction, especially when considering the ECPA’s coverage of e-mails which are transmitted in seconds before being stored on the destination server indefinitely.

<sup>23</sup> Courts have:

[I]nterpreted the ‘interception’ of electronic communications narrowly as extending only to acquisition of the content of such communications during transmission. In order to engage in an improper interception, an employer/supervisor would have to acquire the content of the email during the split second it is being transmitted, or listen into the voice mail message as it is being left for the intended recipient. While this conduct is possible, it is unlikely because employers desiring to monitor e-mail or voice mail on systems they provide need only access the memory where it is stored, rather than the actual transmission itself.

Preeco, Silverman, Green & Egle, P.C., *Articles: Prohibitions Against Monitoring Employee E-Mail And Other Electronic Communications*, available at <http://www.preeosilverman.com/CM/Articles/Articles24.asp> (last visited May 1, 2010).

Exception) or (2) the monitoring occurs in the normal course of business (the Course of Business Exception).<sup>24</sup> The Stored Communications Act does not come to the rescue because it includes the Consent and Course of Business Exemptions and adds another exemption for employers who access stored information if such access is necessary to protect its rights or property as the provider of the electronic service (the Provider Exception).<sup>25</sup> As mentioned previously, both Title I and Title II of the ECPA are ill-equipped to keep pace with the powerful monitoring technologies discussed in Part III.

The Computer Fraud and Abuse Act (CFAA)<sup>26</sup> is a federal law that prohibits “knowingly access[ing] a computer without authorization or exceeding authorized access” and thereby obtaining information or any other thing of value.<sup>27</sup> A few states have passed similar legislation. For example, Virginia prohibits the use of a computer network “without authority” to obtain, embezzle, or otherwise steal property.<sup>28</sup> Under these laws, courts generally hold that “the scope of an individual’s authorization to access a computer network is analyzed ‘on the basis of expected norms of intended use.’”<sup>29</sup> For these reasons, these computer abuse statutes are unlikely to apply to an employer monitoring situations where employers are authorized to access their own property. Instead, these laws are more appropriately used when employees or competitors hack into an employer’s system to discover confidential information.<sup>30</sup>

On the state level, a few jurisdictions have ventured into the electronic monitoring arena - albeit issuing patchwork regulations.<sup>31</sup> For example, California’s constitution creates a right to privacy for its citizens in stating: “[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and

---

<sup>24</sup> 18 U.S.C. § 2511(2)(a)(1) and (d) (2006).

<sup>25</sup> 18 U.S.C. § 2701(c)(1) (2006). “Directed toward protecting a service provider’s normal operations and property, this exception only exempts an employer’s interception ‘incident to the rendition of the company’s services or when the company reasonably believes that the monitoring is necessary to protect its rights or property.’ Thus, it is not difficult for an employer to fall within the . . . exception, considering that it can meet these provisions by showing, for example, that its interception was to protect property (e.g., improper uses or theft) or to provide the service (e.g., quality checks).” Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 297 (April 2002).

<sup>26</sup> 18 U.S.C. § 1030 et seq. (2006).

<sup>27</sup> 18 U.S.C. § 1030(a) (2006). The CFAA applies only when the conduct causes a “loss to [one] or more persons during any [one]-year period . . . aggregating at least \$5,000 in value.” *Id.* at § 1030(a)(5). Losses under the statute include “any reasonable cost to any victim, including the cost of responding to an offense, conducting any damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or consequential damages incurred because of the interruption of service.” *Id.* at § 1030(e)(11).

<sup>28</sup> See VA. CODE ANN. § 18.2-152.3 (2006).

<sup>29</sup> *Global Partners*, *supra* note 21, at 6 (citing *U.S. v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) and concluding that “authorization to access a computer network may not, in some cases, turn simply on a person’s status or position because the ‘expected norms of intended use’ of the network may indicate otherwise.”). This is obviously not the case with the typical employer that monitors a computer network it both pays for and provides to its employees.

<sup>30</sup> See e.g., *Bloomington-Normal Seating Co., Inc. v. Albritton*, U.S. Dist. LEXIS 40302 (C.D. Ill. May 13, 2009) (discussing a case where an employee, among other things, accessed confidential information without authorization and accessed his bosses’ e-mail accounts) and *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int’l. Inc.*, 2009 U.S. Dist. LEXIS 22694 (N.D. Ill. March 19, 2009) (discussing a case under the CFAA where an employee’s actions impaired company data).

<sup>31</sup> See e.g., National Workrights Institute, *Privacy Under Siege: Electronic Monitoring in the Workplace*, 16, available at [epic.org/privacy/workplace/e-monitoring](http://epic.org/privacy/workplace/e-monitoring) (last visited May 1, 2010) [hereinafter *Privacy Under Siege*] (stating that although “some states have shown a willingness to legislate in the employee privacy area, the efforts have only been piecemeal . . . [in fact,] state governments have not addressed the issue comprehensively or uniformly, and in most cases have not addressed it at all.”).

obtaining safety, happiness, and privacy.”<sup>32</sup> California courts have held that this provision applies to private and public employers.<sup>33</sup> As encouraging as this sounds, courts have held that no other state constitution protects an employee’s privacy in a private workplace.<sup>34</sup> On the legislative front, the California Labor Code contains various provisions designed to protect employee privacy in the workplace. One such law requires employers to provide employees and applicants with copies of “any instrument relating to the obtaining or holding of employment” which they are forced to sign.<sup>35</sup> California employers must also disclose in writing certain provisions of the Labor Code before requesting that any employee or applicant take an employment-related test.<sup>36</sup> Additionally, California law prohibits employers from creating audio or video recordings of employees in locker rooms, restrooms, or any other “room designated by an employer for changing clothes, unless authorized by

---

<sup>32</sup> CAL. CONST. art I, § I. Recovery under Article I of the California constitution requires:

First, [the plaintiff] must possess a legally protected privacy interest. These interests include “conducting personal activities without observation, intrusion, or interference”, as determined by “established social norms” derived from such sources as the “common law” and “statutory enactment”. Second, the plaintiff’s expectations of privacy must be reasonable. This element rests on an examination of “customs, practices, and physical settings surrounding particular activities”, as well as the opportunity to be notified in advance and consent to the intrusion. Third, the plaintiff must show that the intrusion is so serious in “nature, scope, and actual or potential impact [as] to constitute an egregious breach of the social norms.”

*Hernandez v. Hillside, Inc.*, 211 P.3d 1063, 1073 (Cal. 2009).

<sup>33</sup> See *Porten v. University of San Francisco*, 64 Cal. App. 3d 825, 829 (Cal. Ct. App. 1976) (holding that the “constitutional provision [Article I, Section I] is self-executing; hence, it confers a judicial right of action on all Californians. Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone.”).

<sup>34</sup> “In all other states, employees have successfully invoked the state constitutional right of privacy only after establishing the government as the employer. Some state courts, such as New Jersey and Alaska, have nevertheless determined that their state constitutions can form a basis for creating public policy arguments in favor of a private sector employee’s right to privacy.” *Privacy Under Siege*, *supra* note 31, at 15. However, as promising as this argument appears, the Alaska Supreme Court has held that “even though an employee drug testing program did not violate the state constitutional right to privacy, public policy favors employee privacy which exists, as ‘evidenced in the common law, statutes and constitution of this state.’ A violation of this policy amounts to a violation of the implied covenant of good faith and fair dealing, and is a wrongful discharge. Therefore, an employee might argue that public policy prohibits employers from monitoring . . . . **As yet, however, no state has ruled to this effect.**” Nathan Watson, *The Private Workplace and the Proposed “Notice of Electronic Monitoring Act”: Is “Notice” Enough?*, 54 FED. COMM. L.J. 79, 91 (2001) (internal citations omitted) (emphasis added).

<sup>35</sup> CAL. LABOR CODE § 432 (West 2002).

<sup>36</sup> CAL. LABOR CODE § 432.2(b) (West 2002).

court order.”<sup>37</sup> In addition, although two notable bills have been introduced in Congress<sup>38</sup>, no federal

---

<sup>37</sup> CAL. LABOR CODE § 435(a) (West 2002). This section also states that “[N]o recording made in violation of this section may be used by an employer for any purpose.” *Id.* at § 435(b). Connecticut has a similar statute. *See* CONN. GEN. STAT. § 31-48b(b) (2008) (prohibiting employers from using electronic surveillance equipment to record employees in areas designed for “health or personal comfort” such as locker rooms, restrooms and break rooms). This law allows for fines for the first and second offenses and then thirty days imprisonment for subsequent offenses. *Id.* § 31-48b(c). This same law also prohibits employers and union representatives from intentionally monitoring conversations concerning labor negotiations unless all parties consent. *Id.* at § 31-48b(d). Connecticut law allows for fines for the first and second offenses and then one year of imprisonment for subsequent offenses. *Id.* at § 31-48b(e). Rhode Island has a similar statute which states that no employer “may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for employees to change their clothes, unless authorized by court order.” R.I. GEN. LAWS § 28-6.12-1 (2007).

<sup>38</sup> The first notable bill to be introduced in the United States Congress was the Privacy for Consumers and Workers Act (PCWA):

On February 27, 1991, the late Senator Paul Simon and Representative Pat Williams introduced the PCWA. The bill would have required employers to clearly define their privacy policies and notify prospective employees of those practices that would affect them. It would have required that surveillance be limited to job related functions and would have prohibited such surveillance of personal communications. It would have prohibited video surveillance in highly personal places such as bathrooms (unless there was suspicion of illegal conduct) and would have required notification when telephone monitoring was taking place. Additionally, it would give employees access to records collected as a result of surveillance.

*Privacy Under Siege*, *supra* note 31, at 19. The second notable bill to be introduced in the United States Congress was the The Notice of Electronic Monitoring Act (NEMA). For more on the NEMA please see *infra* note 37.

law and only two state laws require that notice be provided to employees prior to monitoring.<sup>39</sup> Connecticut<sup>40</sup> and Delaware<sup>41</sup> require that public and private employers provide notice in a conspicuous place of the types of electronic monitoring to be utilized in the workplace. Similar legislation is pending

---

<sup>39</sup> The most recent bill of the two was the Notice of Employee Monitoring Act. It was introduced in nearly identical form in both the House of Representatives and the Senate. See Notice of Electronic Monitoring Act, H.R. 4908, 106th Congress, (2nd Sess. 2000), available at <http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.4908>: (last visited May 1, 2000). It appears that the NEMA died after being referred to the House Committee on the Judiciary and its Subcommittee on the Constitution on July 25, 2000 where hearings were held. See The Library of Congress, THOMAS, H.R. 4908: Notice of Electronic Monitoring Act, available at <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:HR04908:@@L&summ2=m&> (last visited May 1, 2010). A nearly identical bill was introduced in the United States Senate by Senator Charles Schumer. See Notice of Electronic Monitoring Act, S. 2898, 106th Congress, (2nd Sess. 2000), available at <http://thomas.loc.gov/cgi-bin/query/z?c106:S.2898>: (last visited May 1, 2010). It appears that this bill was read twice and then sent to the Senate Judiciary Committee where it died. See The Library of Congress, THOMAS, S. 2898: Notice of Electronic Monitoring Act, available at <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN02898:@@L&summ2=m&> (last visited May 1, 2010).

Generally, the NEMA is a more limited version of the PCWA:

NEMA would have subjected an employer to liability for intentionally monitoring an employee without first having given the employee substantive notice that the employer was engaged in such a monitoring program. Notice fulfilling the requirements of the Act would include the type of monitoring taking place, the means, the type of information that would be gathered including non-work related information, the frequency of monitoring and how the information would be used. An exception to such notice was made if the employer had reasonable grounds to believe the employee was engaged in illegal conduct and surveillance would produce evidence of such. NEMA put no actual restrictions on an employer's ability to monitor as long as they complied with the notice provisions.

*Privacy Under Siege*, supra note 31, at 19. More specifically, this law would have required employers to provide clear and conspicuous notice at all employees that describes:

1. the form of communication or computer usage that will be monitored;
2. the means by which such monitoring will be accomplished and the kinds of information that will be obtained through such monitoring, including whether communications or computer usage not related to the employer's business are likely to be monitored;
3. the frequency of such monitoring; and how information obtained by such monitoring will be stored, used, or disclosed.

*Id.* at § 2(b)(1)-(4). Employers are exempted from the notice requirement when “a particular employee of the employer is engaged in conduct that (A) violates the legal rights of the employer or another person; and (B) involves significant harm to the employer or such other person; and [where] the electronic monitoring will produce evidence of such conduct.” *Id.* at § 2(c)(1)-(2). Aggrieved parties may obtain penalties up to \$5,000 per occurrence and punitive damages and also retain the right to institute a civil action. *Id.* at § 2(d)(1)-(3).

<sup>40</sup> CONN. GEN. STAT. § 31-48d(b)(1) (2008). Connecticut's notice law defines electronic monitoring as “the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, but not including the collection of information . . . for security purposes.” *Id.* at § 31-48d(1)(3). This law also contains an exception from the notice requirement when “an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment and . . . electronic monitoring may produce evidence of this misconduct.” *Id.* § 31-48(b)(2). The law provides for a \$500 penalty for the first offense, a \$1,000 penalty for the second offense and \$3,000 for the third and subsequent offenses. *Id.* at § 31-48d(c).

<sup>41</sup> DEL. CODE ANN. tit. 19 § 705 (2008) (prohibiting employers from monitoring telephone conversations, e-mail usage and Internet usage). There are exceptions to the monitoring prohibition when the employer: (1) provides notice of such monitoring “at least once during each day the employee accesses the employer-provided e-mail or Internet access services or (2) has first given a one-time notice to the employee of such monitoring.” *Id.* at 19 § 705(b). Notice under this statute must be in writing or electronic form and acknowledged by the employee. *Id.* at 19 § 705 (b)(2). This law provides for a \$100 penalty per violation and does not preclude the plaintiff from seeking other remedies. *Id.* at 19 § 705(d).

in Massachusetts,<sup>42</sup> New York<sup>43</sup> and Pennsylvania.<sup>44</sup> Both Colorado and Tennessee require state employers to adopt policies concerning the monitoring of state employee e-mails.<sup>45</sup>

Finally, the common law provides a small amount of protection to employees against excessive monitoring. One of the four so-called “invasion of privacy torts” - intrusion upon seclusion - creates liability when employers invade a place or property where employees have a reasonable expectation of privacy.<sup>46</sup> The Restatement of Torts states that a person is subject to liability for intrusion upon seclusion if the party:

1. Intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, [and]
2. The intrusion would be highly offensive to a reasonable person.<sup>47</sup>

As to the first element of the tort, the defendant must have “penetrated some zone of physical or sensory privacy ... or obtained unwanted access to data” by electronic or other covert means, in violation of the law or social norms. In either instance, the expectation of privacy must be “objectively reasonable.”<sup>48</sup> In addition, this tort requires that the invasion be must be highly offensive to a reasonable person - a difficult standard to meet in the workplace context.<sup>49</sup> This is because electronic monitoring rarely

---

<sup>42</sup> See generally H.R. 1862, 2009 GEN. ASSEM. (Mass. Jan. 13, 2009), available at <http://www.mass.gov/legis/bills/house/186/ht01/ht01862.htm> (containing provisions that would ban monitoring in private workplace areas and require, with exceptions, employers to provide notice to employees as well as the general public before electronic monitoring concerning them takes place (or face a \$5,000 penalty)). Under this pending legislation, employers must also provide employees “with a reasonable opportunity to review and, upon request, a copy of all personal data obtained or maintained by electronic monitoring of the employee.” *Id.* at § 8(a).

<sup>43</sup> A. 3871, 2009-2010, REG. SESS. (N.Y. Jan. 28, 2009) (containing provisions that would require, with exceptions, written notice of electronic monitoring: (1) to be given to employees upon hiring and once each year and (2) to be posted in a conspicuous place). The penalties under this law, if enacted, would be as follows: (1) \$500 for the first offense, (2) \$1,000 for the second offense and (3) \$3,000 for subsequent offenses. *Id.* at § 3(b). It appears that this law died in the New York Senate on January 6, 2010 and was sent back to the New York Assembly when it had its third reading on January 6, 2010. See Sheldon Silver, New York State Assembly, *Bill No. A03871*, available at [http://assembly.state.ny.us/leg/?default\\_fld=&bn=A03871&Summary=Y&Actions](http://assembly.state.ny.us/leg/?default_fld=&bn=A03871&Summary=Y&Actions) (last visited May 1, 2010).

<sup>44</sup> S. 363, 2009, GEN. ASSEM. (Pa. 2009) (requiring written or electronic notice of electronic monitoring in the workplace to be given to and acknowledged by employees). Unlike the laws in Connecticut, Delaware, Massachusetts and New York, Pennsylvania’s law would not provide for a specific penalty; rather, injured parties are allowed to institute private rights of action. *Id.* at § 9(a)(1)-(2). It appears that this bill was last sent to the Communications and Technology Committee of the Pennsylvania Senate on February 20, 2009. See Pennsylvania General Assembly, *Bill Information: Regular Session 2009-2010: Senate Bill 363*, available at <http://www.legis.state.pa.us/cfdocs/billinfo/billinfo.cfm?syear=2009&sind=0&body=S&type=B&bn=0363> (last visited May 1, 2010).

<sup>45</sup> COLORADO REV. STAT. § 24-72-204.5 (2002) and TENN. CODE ANN. § 10-7-512 (2000).

<sup>46</sup> See *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1072 (Cal. 2009) [hereinafter *Hernandez*] (citing cases and stating that a “privacy violation based on the common law tort of intrusion [upon seclusion] has two elements. First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must occur in a manner highly offensive to a reasonable person.”). *Id.* at 1072.

<sup>47</sup> RESTATEMENT (SECOND) OF TORTS § 652B (1977).

<sup>48</sup> *Hernandez*, *supra* note 46, at 1073 (stating that “relevant factors include the degree and setting of the intrusion, and the intruder’s motives and objectives.”).

<sup>49</sup> The second part of the intrusion upon seclusion test is often tough to meet in the employment context because “routine monitoring can appear harmless from some perspectives (especially that of a third party), and because the negative effects of such monitoring are often gradual and incremental, this standard frequently forecloses an employee claim. In particular, when the monitoring complained of has been arguably linked to work-related activities, those challenges have been unsuccessful.” *Under Siege*, *supra* note 31, at 16.

invades places where employees have a reasonable expectation of privacy. In fact, courts have held that a “high threshold must be cleared to assert a cause of action based on [the tort of intrusion upon seclusion].”<sup>50</sup> The Supreme Court has held that the determination of whether an employee has a reasonable expectation of privacy must be made on a case-by-case basis.<sup>51</sup> In one of the few cases where the plaintiff successfully made a case for this tort, a Court held that an employee had a reasonable expectation of privacy in e-mails exchanged with her attorney (sent from her employer provided laptop) from her private, password protected account.<sup>52</sup>

In the end, courts are less likely to find for the plaintiff/employee in these tort suits when the monitoring is conducted on or within employer property as is generally the case. For example, the same court stated that companies:

[C]an adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy.<sup>53</sup>

For the most part, private employers must intrude into very private places - such as restrooms or locker rooms - in order to face liability for intrusion upon seclusion.<sup>54</sup> As demonstrated, this patchwork of state constitutional provisions, state and federal regulations and common law hardly place any restrictions on the to contemporary monitoring techniques discussed next in Part III.

---

<sup>50</sup> *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 678-79 (N.J. 2009) [hereinafter *Loving Care*] (citing cases). Indeed, the “classic conception of this tort, recognized in every state, is that it is used to punish highly offensive privacy invasions. There has been an attempt to apply the tort in the employment context to challenge workplace monitoring abuses. Under present law, however, formidable obstacles face the employee who wishes to bring such a privacy claim.” *Under Siege*, *supra* note 31, at 16.

<sup>51</sup> See *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987) (plurality opinion) (reviewing the tort of intrusion upon seclusion in a lawsuit against a public sector employer).

<sup>52</sup> See *Loving Care*, *supra* note 50, at 687-88 (holding that:

Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care's laptop. Stengart plainly took steps to protect the privacy of those e-mails and shield them from her employer. She used a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer. In other words, she had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit. In light of the language of the Policy and the attorney-client nature of the communications, her expectation of privacy was also objectively reasonable. As noted earlier, the Policy does not address the use of personal, web-based e-mail accounts accessed through company equipment. It does not address personal accounts at all. Nor does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company. Indeed, in acknowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property. Moreover, the e-mails are not illegal or inappropriate material stored on Loving Care's equipment, which might harm the company in some way.)

<sup>53</sup> *Id.* at 692.

<sup>54</sup> See *Williams v. City of Tulsa*, 393 F. Supp. 2d 1124, 1131 (N.D. Okla. 2005) [hereinafter *City of Tulsa*] (stating that “the plaintiffs allege an invasion of their privacy by surveillance in [the workplace] restroom, [various supervisors’ offices], the maintenance shop, the lift station, the weld shop, and various other open areas. Because the Plaintiffs could not show interference with private affairs in other employees’ offices or in open areas generally, the Court concludes that the only allegation the Plaintiffs make that could come within the scope of the tort is that of surveillance in the [workplace] restroom.”).

**Figure 1 – SELECTED STATE WORKPLACE PRIVACY LEGISLATION (ENACTED & PROPOSED)**

WORKPLACE LEGISLATION	PROPOSED IN:	ENACTED IN:
RIGHT TO PRIVACY		CALIFORNIA CONSTITUTION
PRIOR NOTICE OF EMPLOYMENT TESTING		CALIFORNIA
DOCUMENT TRANSMISSION		CALIFORNIA
MONITORING BANNED IN PRIVATE PLACES		5 STATES INCLUDING: CALIFORNIA / CONNECTICUT / NEW YORK / RHODE ISLAND
NOTICE OF ELECTRONIC MONITORING	CALIFORNIA (VETOED) / MASSACHUSETTS / NEW YORK / PENNSYLVANIA	CONNECTICUT / DELAWARE
REQUIRED E-MAIL MONITORING POLICY		COLORADO / TENNESSEE *APPLICABLE TO STATE EMPLOYERS ONLY IN BOTH STATES
INTERCEPTIONS OF ELECTRONIC COMMUNICATIONS - ONLY ONE PARTY NEED CONSENT TO MONITORING		35 STATES INCLUDING: ALABAMA / ALASKA / ARIZONA / ARKANSAS / COLORADO / DELAWARE / GEORGIA / HAWAII / IOWA / KANSAS / KENTUCKY / LOUISIANA / MAINE / MINNESOTA / MISSISSIPPI / MISSOURI / NEBRASKA / NEW JERSEY / NEW MEXICO / NEW YORK / NORTH CAROLINA / NORTH DAKOTA / OHIO / OKLAHOMA / OREGON / RHODE ISLAND / SOUTH CAROLINA / SOUTH DAKOTA / TENNESSEE / TEXAS / UTAH / VIRGINIA / WEST VIRGINIA / WISCONSIN / WYOMING
INTERCEPTIONS OF ELECTRONIC COMMUNICATIONS - ALL PARTIES MUST CONSENT TO MONITORING		12 STATES INCLUDING: CALIFORNIA / CONNECTICUT / FLORIDA / ILLINOIS / MARYLAND / MASSACHUSETTS / MICHIGAN / MONTANA / NEVADA / NEW HAMPSHIRE / PENNSYLVANIA / WASHINGTON
MONITORING OF EMPLOYEES' OUTSIDE ACTIVITIES OR POLITICAL EXPRESSIONS CANNOT LEAD TO ADVERSE ACTION		9 STATES INCLUDING: CALIFORNIA / COLORADO / CONNECTICUT / LOUISIANA / NEW YORK / NORTH DAKOTA / PENNSYLVANIA / SOUTH CAROLINA / WASHINGTON
EMPLOYERS CANNOT MONITOR EMPLOYEES' ASSOCIATIONS, POLITICAL ACTIVITIES, PUBLICATIONS, ETC.		ILLINOIS / MICHIGAN
EMPLOYERS CANNOT MONITOR AND THEN TAKE ADVERSE ACTION BASED ON OFF-DUTY ACTIVITIES	MICHIGAN	4 STATES INCLUDING: CALIFORNIA / COLORADO / NEW YORK / NORTH DAKOTA

WORKPLACE LEGISLATION	PROPOSED IN:	ENACTED IN:
EMPLOYERS CANNOT MONITOR AND THEN TAKE ADVERSE ACTION BASED SPECIFICALLY ON EMPLOYEES' OFF-DUTY USE OF LAWFUL PRODUCTS		<p>9 STATES INCLUDING:  CONNECTICUT / ILLINOIS / MINNESOTA / MISSOURI / MONTANA / NEVADA / NEW MEXICO / NORTH CAROLINA / WISCONSIN  NOTE: RHODE ISLAND'S STATUTE WAS REPEALED</p>
EMPLOYERS CANNOT MONITOR AND THEN TAKE ADVERSE ACTION BASED SPECIFICALLY ON EMPLOYEES' OFF-DUTY USE OF TOBACCO PRODUCTS		<p>16 STATES INCLUDING:  CONNECTICUT / INDIANA / KENTUCKY / LOUISIANA / MAINE / MISSISSIPPI / NEW HAMPSHIRE / NEW JERSEY / NEW MEXICO / OKLAHOMA / OREGON / SOUTH CAROLINA / SOUTH DAKOTA / TENNESSEE / WEST VIRGINIA / WYOMING  *ARIZONA'S STATUTE WAS REPEALED</p>
ANTI-RFID IMPLANTATIONS	MISSOURI / OHIO	NORTH DAKOTA / WISCONSIN
RFID DISCLOSURE, RESTRICTION & DEACTIVATION LAWS	<p>9 STATES INCLUDING:  CALIFORNIA / MASSACHUSETTS / MISSOURI / NEVADA / NEW HAMPSHIRE / NEW MEXICO / RHODE ISLAND / TENNESSEE / WASHINGTON</p>	
RFID STUDY TASK FORCE	<p>4 STATES INCLUDING:  ARKANSAS / MARYLAND / NEW YORK / NEW HAMPSHIRE</p>	
LAWS THAT ENCOURAGE RFID IN SMARTCARDS		TENNESSEE / WASHINGTON

### III. TOP EMPLOYEE MONITORING PRACTICES

Part II demonstrated that the law governing employee monitoring is discombobulated to say the least. This presents a dilemma to employers who navigate the monitoring arena looking for a standardized way to protect their interests. Lacking a clear delineation of best practices, employers have taken a multitude of approaches and monitor their employees in many different ways. For the most part, this monitoring takes place inside the workplace. However, monitoring may also occur outside of the workplace (i.e., GPS tracking of company vehicles or remote e-mail monitoring) or outside of the employment relationship (i.e., investigation of an employee's gambling habits).<sup>55</sup> This section briefly introduces today's most common monitoring practices and how they are implemented into a company's employee monitoring policy.

<sup>55</sup> See e.g., Michael Barbaro, *Bare-Knuckle Enforcement for Wal-Mart's Rules*, N.Y. TIMES, Mar. 29, 2007, at A-1 (discussing situations where Wal-Mart hires private investigators to monitor employees who break work rules - such as co-worker dating - outside of work hours). "Wal-Mart is certainly not the only company, or even the first, to investigate its employees, a practice used widely in corporate America to guard against fraud and protect trade secrets. But despite the retailer's folksy Arkansas image, few companies are as prickly — or unforgiving — about its employees' wayward behavior, a legacy of its frugal founder, Sam Walton, who equated misconduct with inefficiency that would cost customers money." *Id.*

**Figure 3 – TODAY’S TOP CONTEMPORARY MONITORING TECHNIQUES**

ACCESS PANELS	FILTERS & FIREWALLS	SOCIAL NETWORK & SEARCH ENGINE MONITORING
ATTENDANCE & TIME MONITORING	GPS & RFID MONITORING	TELEPHONE & VOICEMAIL MONITORING
AUTOMATIC SCREEN WARNINGS	INTERNET & CLICKSTREAM DATA MONITORING	VIDEO SURVEILLANCE
DESKTOP MONITORING	KEYSTROKE MONITORING	
E-MAIL & TEXT MESSAGE MONITORING	PHYSICAL SEARCHES	

### A. ACCESS PANELS

Access Panels are electronic devices programmed to control entry into a doorway, stairwell, elevator, parking garage, or other restricted area. Typical panels require employees to enter a password, provide a fingerprint/iris scan, or swipe an identification card. Authorized credentials are logged in the system as the panel electronically unlocks the passageway. Unauthorized entry attempts also create a log record and can sound a silent or audible alarm to alert company personnel and/or law enforcement.<sup>56</sup>

Access panels provide key benefits such as:

1. 24-hour employee access to company facilities;
2. The ability to restrict access during specific threats; and
3. The more general ability to secure sensitive areas and information against unauthorized access.<sup>57</sup>

Cisco Systems recently implemented access panel monitoring. The company formed a *Security, Technology and Systems* team tasked with “securely and cost-effectively controlling [access] across the global enterprise.”<sup>58</sup> To this end Cisco employed “[b]adge readers in front of doors or labs or locked

<sup>56</sup> See e.g., NextgenID, *Real-time Event and Alarm Monitoring*, <http://www.nextgenid.com/html/CommandCACS.html> (last visited July 2, 2009) (stating that access panels can perform the following functions related to an alarm:

1. View real-time events for the entire system;
2. View events by building, floor, department, or access panel;
3. View alarms for tailgating, tamper, intrusion, duress, or Watch List incidents;
4. Open an access panel from the System Monitor station; and
5. Lock down an access panel from the System Monitor station).

<sup>57</sup> See e.g., Cisco Systems, *Cisco on Cisco: Physical Security Case Study: How Cisco IT Controls Building Security over the Enterprise WAN*, [http://www.cisco.com/web/about/ciscoitnetwork/security/enterprise\\_network\\_building\\_security\\_web.html](http://www.cisco.com/web/about/ciscoitnetwork/security/enterprise_network_building_security_web.html) (last visited June 28, 2009) [hereinafter *Cisco*] (stating that “[a]fter meeting with executive staff members, a philosophy was defined, which included a primary goal of providing 24-hour access to all Cisco employees. This enabled mobility and higher levels of employee productivity, making it easier for employees to work any time of the day or night while still maintaining physical security.”).

<sup>58</sup> See *id.*

storage rooms, and sometimes even elevators . . . [as well as] [d]oor-latch sensors and controls.<sup>59</sup> This type of access panel monitoring is implemented to increase and stabilize workplace security.

However, access panels can also be used for a different and more extreme level of monitoring - tracking employee behavior. As an example, some employers have been known to place access panels on restroom or break-room doors to monitor how often and for how long employees use these areas.<sup>60</sup> For example, in Pennsylvania, a company allegedly limited employee bathroom breaks to three a day with additional breaks requiring managerial permission.<sup>61</sup> These types of access restrictions are likely legal under Occupational Safety and Health Administration regulations which merely restrict employers from implementing “unreasonable restrictions” on employee restroom use.<sup>62</sup> However, this form of monitoring would be prohibited under the framework detailed in Part IV of this article. Perhaps a more reasonable example occurs when employers in health-sensitive industries, such as restaurants, monitor whether their employees actually wash their hands after using the restroom.<sup>63</sup> Monitoring these activities can play an important part in employer compliance with health regulations but are still designed to monitor employee behavior.

---

<sup>59</sup> See *id.* (stating that “[t]ogether, these technologies help Cisco provide intrusion detection and physical access control. The information they gather is transmitted to centralized security operations centers, where it is reviewed and responded to by the [Security, Technology & Systems] department.”).

<sup>60</sup> See *e.g.*, *When the Boss Doubles as a Bathroom Monitor*, MY LAWYER, <http://www.lawsguide.com/mylawyer/guideview.asp?layer=3&article=160> (reviewing an OSHA inspection of Hudson Foods and stating that:

Hudson workers claim they were required to ask permission before being allowed bathroom breaks -- and that permission was denied as often as granted. Some say they were forced to urinate in their clothes or wear diapers to absorb the inevitable. [A Hudson executive] defended the company's position: The workers simply "need to ask supervisors to release them," he explained. "Normally, a relief person comes by and takes their place." But relief was not always in sight, according to one woman who worked five years as a packer at Hudson. "It matters how good you get along with your supervisor. Sometimes they'll say no," she said. "And it's pretty hard to leave the line when you've got thousands of chickens coming at you.").

Ford Motor Company was disturbed that certain employees at its truck plant in Wayne, Michigan plant were spending more time in the bathroom than their allotted 48 minutes per shift. See *Ford Eyeing Bathroom Breaks: SUV Plant in Michigan to have Supervisors Collect Data on Time Workers Spend in Restroom*, CNN MONEY, Oct. 27, 2005, [http://money.cnn.com/2005/10/27/news/fortune500/ford\\_bathroom\\_breaks/index.htm](http://money.cnn.com/2005/10/27/news/fortune500/ford_bathroom_breaks/index.htm) (reporting that “Ford supervisors will begin collecting weekly data on the amount of time workers spend on bathroom breaks and ‘respond appropriately.’”).

<sup>61</sup> See *e.g.*, Human Resource Blog, *Is it Legal to Restrict Workplace Bathroom Visits to a Certain Number Per Day??*, Apr. 2, 2009, <http://www.humanresourceblog.com/2008/04/02/is-it-legal-to-restrict-workplace-bathroom-visits-to-a-certain-number-a-day/> (discussing a program where an employee’s key card would allow access to the restroom three times per day and then block additional access). This company allegedly enforced this policy by programming access panels to allow access up to three times and then deny access thereafter. *Id.*

<sup>62</sup> See John B. Miles, Jr., *OSHA Interpretation of 29 C.F.R. § 1910.141(c)(1)(i): Toilet Facilities*, Apr. 6, 1998, available at [http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=INTERPRETATIONS&p\\_id=22932](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=INTERPRETATIONS&p_id=22932) (interpreting OSHA regulations regarding use and condition of toilet facilities).

<sup>63</sup> See *e.g.*, *Hand Washing Monitor*, FRESH PATENTS, <http://www.freshpatents.com/-dt20090226ptan20090051545.php> (last visited July 2, 2009) (describing a patent application for a hand washing monitor that operates as follows:

A person is detected entering a room and an image of the person is captured. The person is identified as an employee using various employee identifiers or is identified as a visitor. The image may be used to identify distinguishing features of the visitor to be compared to an image subsequently during hand washing to verify the identity of the hand washer as the person who entered the room. Similarly, the employee identifier is used to verify the identity of a hand washer as the employee that entered the room. If any person entering the room remains for a threshold period of time without activating the soap dispenser, then a notification that includes the person's identity is provided within the room to remind the person that hand washing is required.).

## B. ATTENDANCE AND TIME MONITORING

It is an understatement to claim that attendance is a key component of workplace productivity. Workers who fail to show up on time, leave early or miss extended amounts of time are also liabilities from a monetary and legal standpoint. A recent study showed that employee absences comprise 36% of payroll expenses<sup>64</sup> or approximately \$100 billion a year nationwide.<sup>65</sup> Most of these costs stem from hiring substitute workers and/or paying overtime to current employees in order to complete assigned tasks.<sup>66</sup> However, perhaps a more important cost associated with absenteeism is the negative effect it has on customer satisfaction, other employees, team chemistry and productivity.<sup>67</sup> With this in mind, employers are wise to expend actual and political capital monitoring employee attendance.

The secret to attendance monitoring is to capture the amount of time missed as well as patterns and reasons for absences among individuals, teams and departments. This type of attendance monitoring can be either physical (via a time clock) or electronic (via “in and out” monitoring software installed on computers). There is even a formula - called the Bradford Factor - that looks at spells of absences multiplied by days missed during each spell.<sup>68</sup> The higher the score, the more disruptive each absence is to the company.

It is more efficient to monitor employee hours via software as opposed to on paper as it reduces hours inflation and human errors. Attendance software is programmed to monitor attendance patterns and trends to determine which employees may be excessively absent or taking advantage of the system.<sup>69</sup> This software can cross-reference employee attendance rates across department and alert employers to problem areas.<sup>70</sup> Employers can be required to enter the reason behind their absence which can help

---

<sup>64</sup> See Kronos, *Workforce Timekeeper: Overview*, <http://www.kronos.com/Absence-Management/Absence-Management-Software.aspx> (last visited June 28, 2009) [hereinafter *Workforce Timekeeper*] (stating that this figure comprises the cost of paying absent employees, lost productivity and the hiring of replacement employees).

<sup>65</sup> See Marcia Carruthers and Nazeen Vimadalal, *Double Whammy of Absence Costs has Employers Searching for Answers*, 23 EMPLOYEE BENEFIT NEWS 7, 49 (June 2009). This is up from approximately \$74 billion annually in 2006. See Gina Ruiz, *Tallying the Cost of Absenteeism*, WORKFORCE MANAGEMENT, Apr. 19, 2006, <http://www.workforce.com/section/00/article/24/33/85.html> [hereinafter *Absenteeism*]. The average annual “per-employee cost of of absenteeism” is around \$700. See e.g., Braun Consulting News, *Absenteeism and the Bottom Line*, Winter 2003, <http://www.braunconsulting.com/bcg/newsletters/winter2003/winter20032.html> (citing various studies on employee absenteeism and stating, however, that the per employee cost of absenteeism has been decreasing in the United States since 2000).

<sup>66</sup> See *id.*

<sup>67</sup> See *id.*

<sup>68</sup> See e.g., *Reducing and Managing Workplace Absenteeism*, BNET, [http://www.bnet.com/2410-13056\\_23-59947.html](http://www.bnet.com/2410-13056_23-59947.html) (last visited July 7, 2009) [hereinafter *Workplace Absenteeism*] (defining the Bradford Factor as equalling  $S \times \bar{S} \times D$ :

[W]here S is the number of spells of absence over the last year and D is the number of days absent in the same period. For example, if an employee is absent for one period of 15 days (such as missing three continuous work weeks), the score is  $1 \times 1 \times 15 = 15$  points. In contrast, if he or she was absent for 15 days on 15 separate occasions spread out over the course of the year, the same person’s score would be  $15 \times 15 \times 15 = 3,375$  points.).

<sup>69</sup> See e.g., *Workforce Timekeeper*, *supra* note 64 (claiming that managers must “control the impact of absenteeism . . . manage [policies to] minimize compliance risk [and] identify workers with attendance issues so you can improve workforce productivity.”).

<sup>70</sup> See e.g., PATRICIA BOOTH, EMPLOYEE ABSENTEEISM: STRATEGIES FOR PROMOTING AN ATTENDANCE-ORIENTED CORPORATE CULTURE, 6 (Conference Bd. of Canada 1993), available at <http://as01.ucis.dal.ca/hrd/files/attend.pdf> [hereinafter EMPLOYEE ABSENTEEISM].

employers implement solutions.<sup>71</sup> Additionally, attendance software can also quickly and correctly calculate pay and other legally mandated work provisions<sup>72</sup> under the Fair Labor Standards Act,<sup>73</sup> Family and Medical Leave Act<sup>74</sup> and various state laws.<sup>75</sup> Finally, such software frees up administrative time for human resources employees to concentrate on other tasks. Typical attendance monitoring is not invasive and even expected by employees.

### C. AUTOMATIC SCREEN WARNINGS

Automatic Screen Warnings are disclaimers which load automatically onto employee screens before the system grants access to the requested program. These warnings are intended to inform employees that they are being or may be monitored. Such screens can be customized to list each item that the employer monitors or employers can limit the disclosure to the monitoring about to take place.<sup>76</sup> Automatic screen warnings can be an important for compliance with a company policy that promises to disclose monitoring practices before they take place. It is important to note that automatic screen warnings are not required before monitoring takes place. In fact, one court has held that employers who breach their promises not to monitor without such notice may still do so without violating any employees' right to privacy.<sup>77</sup> The prudent course, however, is to adhere to such promises or not make them at all. Such

---

<sup>71</sup> *Id.* In addition when “managers and others show that they’re interested and will follow up with individuals with high rates of absenteeism, ‘sickness’ rates almost always decline.” *Workplace Absenteeism*, *supra* note 68.

<sup>72</sup> See e.g., *Workforce Timekeeper*, *supra* note 64 (stating that this software can also create employee shifts and schedules).

<sup>73</sup> 29 U.S.C. § 201 et seq., § 206, § 207 & § 211 (2006) (discussing requirements surrounding minimum wage, maximum hours and record keeping requirements).

<sup>74</sup> 28 U.S.C. § 2601 et seq., § 2611 and § 2612 (2006) (defining covered employees and discussing employee entitlement to family and or medical leave based on months and hours worked).

<sup>75</sup> Additionally, wise supervisors keep time records accurately to prevent losing their own jobs. See e.g., Jaime Powell, *Why You Should do a Reality Check when Reviewing Timesheets*, EMPLOYER LAW REPORT, Jan. 30, 2009, available at <http://www.employerlawreport.com/2009/01/articles/wage-hour/why-you-should-do-a-reality-check-when-reviewing-timesheets/> (discussing the firing of a supervisor who failed to monitor the accuracy of a subordinate’s time sheets when the subordinate logged time spent at a casino as work time).

<sup>76</sup> Brian Levine, Commentary: *E-mail your Client at Work, Kiss Privilege Goodbye*, KANSAS CITY DAILY NEWS-PRESS, Feb. 28 2006, available at [http://findarticles.com/p/articles/mi\\_qn4181/is\\_20060228/ai\\_n16202823/](http://findarticles.com/p/articles/mi_qn4181/is_20060228/ai_n16202823/) (discussing the intersection of attorney-client privilege and employer monitoring and stating that employees’ “computers might present a warning screen when the user logs on, or emails may be sent with an automatic footer indicating that the email is the property of the corporation.”).

<sup>77</sup> *Smyth v. Pillsbury*, 914 F. Supp. 97, 98 & 101 (E.D. Pa. 1996) (discussing the employer’s policy that e-mail messages would not be used as grounds for termination and reprimand and holding that:

[E]ven if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. Again, we note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.)

notice will help defeat any reasonable expectation of privacy an employee has in any given electronic activity.<sup>78</sup>

#### D. DESKTOP MONITORING PROGRAMS

Desktop monitoring programs can obtain every command and keystroke sent to the desktop by a user, translate these signals into data and remotely transmit this information to the employer.<sup>79</sup> Desktop monitoring programs can be installed physically or remotely via a “trojan horse” e-mail attachment.<sup>80</sup> These programs can record and copy, in real-time, the following activities which occur on an employee’s desktop:

1. **APPLICATION TRACKING** - tracks which software applications are used and for how long;
2. **DOCUMENT TRACKING** - tracks each document accessed on an individual computer;
3. **EVENTS TIMELINE** - tracks the order in which employees work on assignments;
4. **LOG-ON MONITORING** - tracks how often and when employees log-on to employer’s system;
5. **PASSWORD LOGGING** - tracks any passwords entered over the employee’s computer;
6. **PRINT JOBS EXECUTED** - tracks individual print requests;
7. **SCREENSHOT CAPTURE** - tracks information on an employee’s screen at any given time;
8. **SOFTWARE INSTALLATION** - tracks any software loaded onto an employee’s computer; and
9. **WINDOW ACTIVITY** - tracks all windows opened per session.<sup>81</sup>

#### E. E-MAIL MONITORING

---

<sup>78</sup> See e.g., *United States v. Greiner*, 235 Fed. Appx. 541, 542 (9th Cir. 2007) (discussing a case of an employee’s claim that his employer’s remote Internet monitoring violated the Fourth Amendment and holding that:

The warning banner confronting [the plaintiff/employee] every time he logged onto his computer gave him ample reason to be aware that his stored files and internet usage were subject to monitoring by his employer and disclosure to law enforcement personnel, and that by using the computer he was deemed to have consented to such monitoring and disclosure. Thus, [the plaintiff/employee] lacked a legitimate expectation that his internet activity would remain private from his employer.)

and *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (stating that “privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user [i.e. via an automatic screen warning.]”). See also William A. Herbert, Symposium: *The Electronic Workplace: To Live Outside the Law you Must be Honest*, 12 EMPL. RTS. & EMPLOY. POL’Y J. 49, 60-61 (2008) (stating that “automatic screen warnings, upon logging in, can help to ensure that an employee’s subjective expectation of privacy will be found unreasonable by a court.”).

<sup>79</sup> Kevin Bonsor, *Is your Workplace Tracking your Computer Activities?*, HOW STUFF WORKS, <http://computer.howstuffworks.com/workplace-surveillance3.htm> (last visited July 14, 2009) [hereinafter *Workplace Tracking*] (describing desktop monitoring as follows: “Every time you provide some form of input for your computer, whether it’s typing on the keyboard or opening a new application, a signal is transmitted. These signals can be intercepted by a desktop monitoring program, which can be installed on a computer at the operating system level or the assembly level. The person receiving the intercepted signals can see each character being typed and can replicate what the user is seeing on his or her screen.”).

<sup>80</sup> See *id.* (defining a trojan horse as a “desired program [usually sent as an e-mail attachment by an employer to an employee] that contains an undesired program” and stating that desktop monitoring programs can be physically installed onto the employee’s computer or delivered remotely via a trojan horse.).

<sup>81</sup> See e.g., Computer Monitoring, *Employee Monitoring Software: NetVisor*, [http://www.computer-monitoring.com/employee\\_monitoring.htm](http://www.computer-monitoring.com/employee_monitoring.htm) (last visited June 28, 2009) [hereinafter *Computer Monitoring*].

Monitoring e-mail accounts is a common practice and over 40% of all employers monitor at least a portion of their employee e-mail accounts.<sup>82</sup> This form of monitoring is generally implemented via software programs capable of tracking the content, timing, volume and recipients of sent and received e-mail.<sup>83</sup> These sophisticated programs can even track an employee's Web-based e-mail accounts provided by, for example, America Online, Hotmail or Yahoo - personal accounts that employees often assume are off-limits to monitoring.<sup>84</sup> The extent of such tracking is large in scope as over 60 million employees have e-mail and/or Internet access at work.<sup>85</sup> 96% of employers who monitor e-mail track external - incoming and outgoing - e-mails.<sup>86</sup>

Employers monitor their employees' e-mail for a multitude of reasons, the most important being to: (1) check in on productivity, (2) look for sexual harassment/sex discrimination and workplace violence<sup>87</sup> (3) look for offensive language and/or pornography and (4) monitor language for transmission of trade secrets or other confidential information.<sup>88</sup> Such monitoring can help lower legal liability.<sup>89</sup> 28% of employers who monitor e-mail have admitted to terminating at least one employee because of inappropriate e-mail.<sup>90</sup> Most of these terminations were for violating company policy (64%) generally

---

<sup>82</sup> 2007 *Electronic Monitoring & Surveillance Survey*, AM. MGMT. ASS'N, at 4, Feb. 28, 2008, available at <http://www.plattgroupinc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf> [hereinafter *2007 AMA Survey*] (stating that 26% of employers monitor all employees' e-mail accounts, while 17% of employers only monitor the e-mail accounts of employees in selected job categories).

<sup>83</sup> 2007 *AMA Survey*, *supra* note 2, at 5 (stating that 73% of all employers who monitor employee e-mails do so via software monitoring programs).

<sup>84</sup> *Online Spying: Remote Computer Spyware Software*, ONLINE SPYING, <http://www.online-spying.com/webmail-spy.html> (last visited July 14, 2009) (stating that the Spy software program:

[A]llows you to record ALL e-mail sent and received on your computer - bar none! With WebMail Spy's advanced, foolproof and secure monitoring system, all e-mail sent via Outlook, Outlook Express, Eudora, Netscape (to name a few) will be recorded. On top of that, WebMail Spy will also record all Incoming AND Outgoing e-mail (POP3/SMTP e-mail's), ALL America Online e-mail's, and ALL web based e-mail - for services such as HotMail, Yahoo! Mail, mail2web, and many more.)

See also Rachel Konrad and Sam Ames, *Web-Based E-mail Services Offer Employees Little Privacy*, CNET NEWS, Oct. 3, 2000, <http://news.cnet.com/2100-1017-246543.html> (stating that "unfortunately, security experts say many employees would be surprised to know that Web-based email services also offer little privacy. Messages sent via a Yahoo or Hotmail account . . . are just as accessible [as employer-created e-mail accounts] to nosy employers.").

<sup>85</sup> See e.g., Marc A. Sherman, *Webmail at Work: The Case for Protection Against Employer Monitoring*, 23 *TOURO L. REV.* 647, 656 (2007) [hereinafter *Webmail at Work*] and Mary Madden and Sydney Jones, *Networked Workers: Most Use Email, but say Technology is a Mixed Blessing*, PEW INTERNET & AM. LIFE PROJECT, Sept. 24, 2008, <http://pewresearch.org/pubs/966/networked-workers>.

<sup>86</sup> 2007 *AMA Survey*, *supra* note 2, at 1.

<sup>87</sup> See e.g., Ann Carns, *Prying Times: Those Bawdy E-Mails Were Good for a Laugh -- Until the Ax Fell*, *WALL ST. J.*, Feb. 4, 2000, at A1 (discussing a lawsuit brought against Chevron employees accusing the company of allowing sexually harassing e-mails to be sent and received on company accounts; Chevron settled the claim for \$2.2 million). The e-mails in question contained a story entitled "25 Reasons Why Beer is Better than Women." See *JOKES AND HUMOR.COM*, <http://www.jokesandhumor.com/jokes/137.html> (last visited July 17, 2009).

<sup>88</sup> See e.g., 2007 *AMA Survey*, *supra* note 2, at 1 and Thomas J. Harvey, *Beware Workplace E-Mail, Survey Says*, ASAE & THE CENTER FOR ASSOCIATION LEADERSHIP, 2001, available at <http://www.asaecenter.org/PublicationsResources/whitepaperdetail.cfm?ItemNumber=12168> (stating that 8% of companies in a recent survey claimed that they had battled a sexual harassment or sex discrimination lawsuit based on employee e-mail or Internet use.). See also *Webmail at Work*, *supra* note 85, at 651 (stating that a "short list of other risks [of not monitoring employee e-mail] includes compromise of sensitive or proprietary information, damage to public image, and vicarious liability for various torts.").

<sup>89</sup> See e.g., 2007 *AMA Survey*, *supra* note 2, at 1-2 (stating that the "failure to monitor internal e-mail is a potentially costly oversight, as employees tend to play it fast and loose with internal e-mail, transmitting jokes, gossip, disparaging remarks, pornography, and other content that triggers workplace lawsuits.").

<sup>90</sup> See 2007 *AMA Survey*, *supra* note 2, at 1.

based on inappropriate and offensive language/content; other terminations were based on excessive personal use of the Internet while at work (26%) and breach of confidentiality (22%).<sup>91</sup> As discussed previously, e-mail monitoring is generally legal - with or without prior employee notification.<sup>92</sup>

## F. FILTERS & FIREWALLS RESTRICTING INTERNET ACCESS

Filters and firewalls not only prevent outsiders from gaining access to an employer's system - they also can be used to prevent employees from accessing information or Web sites unrelated to work. This firewall is designed to make employees more productive and stop non-work related activities during work hours. To this end, 65% of employers block unauthorized or inappropriate Web sites on employee computers.<sup>93</sup> The vast majority of such filters block Web sites categorized as adult with "sexual, romantic [and/or] pornographic content."<sup>94</sup> Filters also block Web sites dedicated to gaming,<sup>95</sup> social networking,<sup>96</sup> entertainment,<sup>97</sup> shopping<sup>98</sup> and sports.<sup>99</sup> 18% of employers filter out external blogs as well.<sup>100</sup> The effectiveness of this monitoring program can be questioned as most employees can access prohibited sites from their personal PDA or smartphone thereby circumventing the employer's firewalls and filters.

## G. GPS, RFID & SMARTCARDS

Global Positioning Systems (GPS) and Radio Frequency Identification Devices (RFID) are electronic tracking devices. This technology provides precise location information of objects or individuals on a real-time basis by triangulating satellite signals.<sup>101</sup> Employers utilize these tracking devices to monitor the whereabouts of their employees and property. It is important to note that GPS and RFID devices are not solely designed to monitor vehicles; these devices often monitor employee cell phones, laptops, PDAs and Smartcards or other forms of employer property.<sup>102</sup> Employers also use this technology to authorize the operation of equipment, track their employees location within the workplace, and even

---

<sup>91</sup> 2007 AMA Survey, *supra* note 2, at 8-9.

<sup>92</sup> Encouragingly, 71 percent of employers monitoring employee e-mail notify such employees prior to any monitoring. See 2007 AMA Survey, *supra* note 2, at 5 (stating that 11 percent of employers do not notify employees while another 18 percent do not know whether e-mail monitoring took place).

<sup>93</sup> See 2007 AMA Survey, *supra* note 2, at 5.

<sup>94</sup> See 2007 AMA Survey, *supra* note 2, at 5 (stating that 91% of implemented filters block adult content).

<sup>95</sup> See *id.* at 5-6 (stating that 61% of implemented filters block gaming Web sites).

<sup>96</sup> *Id.* at 5-6 (stating that 50% of implemented filters block social networking Web sites).

<sup>97</sup> *Id.* at 5-6 (stating that 40% of implemented filters block entertainment Web sites).

<sup>98</sup> *Id.* at 5-6 (stating that 27% of implemented filters block shopping or on-line auction sites).

<sup>99</sup> *Id.* at 5-6 (stating that 21% of implemented filters block sports Web sites).

<sup>100</sup> *Id.* at 6.

<sup>101</sup> William A. Herbert and Amelia K. Tuminaro, Symposium: *Emerging Technology and Employee Privacy: The Impact of Emerging Technologies in the Workplace: Who's Watching the Man (Who's Watching Me)?*, 25 HOFSTRA LAB. & EMP. L.J. 355, 370 (Spring 2008) [hereinafter *Emerging Technology*] (internal citations omitted).

<sup>102</sup> See e.g., *Emerging Technologies*, *supra* note 101, at 370.

determine if employees are working the amount of hours claimed on time sheets.<sup>103</sup> This technology can also be used to produce real-time reports on employee productivity and encourage competition among employees to be more productive.<sup>104</sup>

At an extreme level, employers have yet to make a push to implant RFID chips into employees for monitoring purposes. Before brushing this idea off as unrealistic, take note that three states - Wisconsin,<sup>105</sup> North Dakota<sup>106</sup> and California<sup>107</sup> - recently passed laws prohibiting employers from requiring, coercing, or compelling employees to receive RFID implants. Some argue that these statutes do not go far enough to effectively prevent RFID devices from being implanted or ingested.<sup>108</sup> For example, RFID trackers can be swallowed rather than implemented thus bringing this practice outside of the state laws.<sup>109</sup> Also, these statutes ban forced implementation allowing RFID to be voluntarily implemented in exchange for a financial reward.<sup>110</sup> GPS and RFID monitoring is new and, therefore, lacks settled statutory coverage and judicial precedent.<sup>111</sup> Tracking devices can pose a major privacy

---

<sup>103</sup> See e.g., Jeffery Barker, *Businesses use RFID to Track Workers, Pay for Fewer Hours*, Jan. 14, 2009, MEDILL REPORS (NORTHWESTERN UNIVERSITY, CHICAGO), available at <http://news.medill.northwestern.edu/chicago/news.aspx?id=111561> [hereinafter *RFID*] (stating that the “same computer chips used to track razor blades and lipstick are now being used to track workers and cut jobs.”). In fact, retailers, “such as Wal-Mart and Target, have used the technology to track their products [but, with the same technology also can] track how quickly employees are working and then pay them for fewer labor hours.” *Id.*

<sup>104</sup> See *id.* (stating that companies are also using RFID “to track how quickly employees work and have them compete with each other in order for everyone to work faster. If a task normally takes two minutes and an employee finds a more efficient way to get it done in one minute, then the standards are changed.”).

<sup>105</sup> WIS STAT. § 146.25 (2008) (stating that: (1) No person may require an individual to undergo the implanting of a microchip [and] (2) Any person who violates sub. (1) may be required to forfeit not more than [\$]10,000. Each day of continued violation constitutes a separate offense.”).

<sup>106</sup> N.D. CENT. CODE § 12.1-15-06 (2009) (stating that “[a] person may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device. A violation of this section is a class A misdemeanor.”).

<sup>107</sup> CAL. CIV. CODE § 52.7(a) (Deering 2009) (stating that, with certain exceptions, “a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device.”). More specifically, this statute defines the phrase “require, coerce, or compel” to include “physical violence, threat, intimidation, retaliation, the conditioning of any private or public benefit or care on consent to implantation, including employment, promotion, or other employment benefit, or by any means that causes a reasonable person of ordinary susceptibilities to acquiesce to implantation when he or she otherwise would not.” *Id.* at 52.7(h)(4).

<sup>108</sup> See e.g., Marc L. Songini, *N.D. Bans Forced RFID Chipping*, COMPUTER WORLD, Apr. 12, 2007, [http://www.computerworld.com/s/article/9016385/N.D.\\_bans\\_forced\\_RFID\\_chipping?taxonomyId=15&intsrc=hm\\_topic](http://www.computerworld.com/s/article/9016385/N.D._bans_forced_RFID_chipping?taxonomyId=15&intsrc=hm_topic).

<sup>109</sup> See *id.* (interviewing a professor specializing in computer issues who discussed the North Dakota statute and stated that “the law is too vague to do much good. For instance, it only addresses situations where a chip is injected, even though RFID tags can also be swallowed.”).

<sup>110</sup> See *id.* (quoting a computer expert who mentioned that these laws tend not to “clearly define what a forced implant really is; someone could make chipping a requirement for a financial reward. ‘Suppose I offer to pay you \$10,000 if you have an RFID [chip] implanted?’ [pondered the expert]. ‘Is that ‘requiring’ if it's totally voluntary on your part?’ The idea behind the law isn't bad, but ‘it looks hastily drawn and will have unpredictable consequences.’”).

<sup>111</sup> Although not in an employment context, California has enacted a statute prohibiting rental car companies from utilizing data gathered from GPS devices installed in rental cars except to repair a defect in the GPS device itself. CAL. CIV. CODE § 1936(o)(1)(B)(3) (Deering 2009). Perhaps this is an early prediction as to how the California Legislature might view GPS tracking in the workplace. Texas makes it a crime to install a GPS tracking device in a motor vehicle that the installer does not own. TEX. PENAL CODE ANN. § 16.06(b) (Vernon 2009) (stating a few affirmative defenses none of which mention employers directly). Under this Texas law, however, it would not be illegal for an employer to install a GPS tracking device on its own vehicles which are driven by its employees. Employers would violate the law by installing tracking devices on their employees' personal vehicles.

invasion if employers utilize them to track off-duty behavior. On the other hand, employers can claim that off-duty behavior can negatively impact on-duty performance and company reputation.

Finally, A SmartCard is generally a plastic identification card embedded with a microchip allowing it to function as much more than just an ID. The following defines how a large company monitors its employees with smart identification badges:

Cisco has a database of all its employee records that is updated when an employee joins or leaves Cisco. After a background check, new employees are added to the database, and go to the local Cisco security office to obtain a badge with their picture on it. Badges are unique to each employee, and can be used only at Cisco locations. Not only is the employee's picture on the badge, but the embedded badge number is used to identify the employee every time the badge is used to open a door. The picture is copied from the regional security server to the global enterprise system, and also copied to the employee directory where it is available to all employees.<sup>112</sup>

## **H. INTERNET USE AUDITS (INTERNET MONITORING)**

Otherwise known as Internet monitoring, Internet Use Audits track an employee's Web activity over a period of time. Employers utilize this technology to determine employee productivity and to check for inappropriate activities. 30% of employers have terminated an employee for unauthorized Internet use.<sup>113</sup> 84% of such terminations were at least partially based on an employee's viewing or downloading inappropriate and/or offensive content.<sup>114</sup>

Internet Use Audits can be minimal, moderate or all-encompassing. Minimal audits occur when employers collect anonymous data on which Web sites their employees view. These reports may be used to set or amend current Internet Use policies. Moderate audits are a bit more intrusive and analyze specific Web sites visited by individual employees during work hours. All-encompassing Internet Use Audits occur when employers collect and mine clickstream data. Clickstream data are the "electronic footprints created when a Web user moves about in cyberspace."<sup>115</sup> Clickstream technology records each mouse click on each Web page visited as a user navigates the World Wide Web.<sup>116</sup> Clickstream data can be "shockingly revealing, providing a record of the entirety of one's online experience, including movements among Web sites, geographical location, the type of computer and Internet browser in use, and any transactions or comments made at individual Web sites."<sup>117</sup> Clickstream monitoring allows employers to accurately recreate entire periods (i.e., specific days, quarters, projects) and determine employee productivity, focus and adherence to company policy.

---

<sup>112</sup> *Cisco*, *supra* note 57.

<sup>113</sup> *See 2007 AMA Survey*, *supra* note 2, at 9.

<sup>114</sup> *See id.*

<sup>115</sup> Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 61 (2000) [hereinafter *Establishing a Legitimate Expectation*].

<sup>116</sup> Clickstream data is more often collected by Internet retailers to monitor, data mine and predict consumer desires and purchasing behavior. *See e.g. Establish a Legitimate Expectation*, *supra* note 115, at 65 (stating that an "increasing number of private companies are monitoring, recording, and analyzing clickstreams in an effort to make Internet advertising more effective.").

<sup>117</sup> *Establishing a Legitimate Expectation*, *supra* note 115, at 64-65.

Finally, contemporary employees are becoming more capable when it comes to: (1) creating their own blogs and (2) posting their thoughts on a social networking Web site. Unhappy employees have been known to utilize these forums to focus on particular workplace issues - and often times do not realize or believe that their employer will ever see the content.<sup>118</sup> However, 74% of employees believe that it is relatively easy to damage a company's reputation via a blog or a social networking Web site.<sup>119</sup> Employers often struggle formulating policies to govern such blogs - particularly when such blogs go negative. The tension is not only between employee privacy versus employer interests but also involves an individual's personal expressions.<sup>120</sup> Regardless, a small minority of employers - around 12% - have begun to monitor employee blogs and employee postings on social networking Web sites.<sup>121</sup> Although an even smaller percentage of employees have been terminated based on blog activity, under 0.5%,<sup>122</sup> there is a term of art to describe the process - being "dooced."<sup>123</sup> This term stems from the actual termination of an individual employee for creating a personal blog - located at [www.dooce.com](http://www.dooce.com) - which included comments critical of management.<sup>124</sup> Such monitoring is likely legal, although some states have enacted statutes prohibiting employers from disciplining or terminating employees for their off duty conduct such as drinking, smoking, or posting on blogs/social networking Web sites.<sup>125</sup> Although

---

<sup>118</sup> See e.g., Moran Dwyer and Jennifer G. Knight, *Monitoring Employee Blogs: Unanticipated Costs and Risks*, CROWELL MORING, May 2006, <http://www.crowell.com/NewsEvents/Article.aspx?id=247> [hereinafter *Monitoring Employee Blogs*] (stating that "[F]or their part, employees often assume that their employers will never read their blogs, which may be why they feel free to criticize their employers openly. Blogs exist in the public forum, however, and there is no guarantee that an employer will not run across an employee's blog.").

<sup>119</sup> See e.g., Deloitte, *Social Networking and Reputation Risk in the Workplace*, 2009, at 4, available at [http://www.deloitte.com/dtt/cda/doc/content/us\\_2009\\_ethics\\_workplace\\_survey\\_220509.pdf](http://www.deloitte.com/dtt/cda/doc/content/us_2009_ethics_workplace_survey_220509.pdf) [hereinafter *Social Networking*]. At the same time, 58% of executives believe that reputational risk stemming from negative comments on social networking Web sites should be a board room issue. *Id.* at 5 (stating that only 15% of companies actually make such risks a board room issue).

<sup>120</sup> See *id.* (stating that when it "comes to blogging, it is difficult for employers to draw lines between protecting their legitimate interests and respecting employees' expression of personal opinions."). The same is also true of employees' expression of personal opinions on social networking Web sites. Employers should also look at the size of the blog's audience to determine the potential impact. However, smaller audiences do not necessarily indicate low impact considering how quickly blog content can spread online.

<sup>121</sup> See *id.* at 6 (stating that 12% of employers monitored "the blogosphere to see what is being written about it" while 50% claimed that they did not and 38% were not sure whether such monitoring was taking place). In addition, 10% of employers regularly monitor social networking Web sites to see what is being said about it. *Id.*

<sup>122</sup> See *2007 AMA Survey*, *supra* note 2, at 9 (stating that 0.4% of organizations have fired an employee for a posting on a personal blog).

<sup>123</sup> Heather Armstrong was terminated after a supervisor was alerted to her personal blog - located at [www.dooce.com](http://www.dooce.com) - that contained comments critical of management. See e.g., *Monitoring Employee Blogs*, *supra* note 118.

<sup>124</sup> See *id.*

<sup>125</sup> See e.g., N.Y. LAB. LAW § 201-d(2)(c) (McKinney 2002) (prohibiting discrimination, refusal to hire, or termination of employees based on "legal recreational activities outside work hours, off of the employer's premises and without use of the employer's equipment or other property") and COLO. REV. STAT. § 24-34-402.5(1) (2008) (prohibiting termination of employees "due to that employee's engaging in any lawful activity off the premises of the employer during nonworking hours"). In addition, punishment stemming from blog or social networking content may violate state and/or federal whistleblowing statutes if the employee posts about illegal conduct in order to disclose such conduct to the government. See e.g., CAL. LAB. CODE § 1102.5(a) (Deering 2009) (stating that an employer "may not make, adopt, or enforce any rule, regulation, or policy preventing an employee from disclosing information to a government or law enforcement agency, where the employee has reasonable cause to believe that the information discloses a violation of state or federal statute, or a violation or noncompliance with a state or federal rule or regulation."). Employers have much more leverage if the blogging occurs during work hours as these recreational activity statutes would not apply.

many of these laws contain an employer exception allowing such discipline if the outside of work activity is rationally related to work activities.<sup>126</sup>

## I. KEYSTROKE LOGGING

Also called key-logging, this form of monitoring occurs when individual key strokes are recorded/logged and made accessible to others. Logging occurs via a hardware device physically attached to the user's computer or a software program installed on a user's computer. Logging programs allow employers to enter a password and convert keyboard-based activities into text. These results are used to determine employee effectiveness and productivity. As with most types of employee monitoring keystroke logging is generally done in secret to obtain more accurate results.<sup>127</sup>

Key-logging is a risky practice as it can be construed as an interception of electronic communications in violation of the ECPA.<sup>128</sup> Two key questions arise when considering this issue: (1) does key-logging constitute an interception under the ECPA and (2) do such interceptions affect interstate commerce as required by the ECPA? A recent federal district court case in California recently addressed both questions. In *Brahmana v. Lembo* an employee sued his employer under the ECPA for intentionally logging his keystrokes, obtaining the password to a personal e-mail account and accessing such account.<sup>129</sup> The court determined that electronic information was intercepted - even if it only occurred between the keyboard and the computing processing unit.<sup>130</sup> This is a controversial position because an argument can be made that electronic communications are merely prepared when typed and then transmitted later when the user sends an e-mail, instant message, etc.<sup>131</sup> As to the second question, the *Lembo* court avoided determining whether intercepting key strokes affects interstate commerce.<sup>132</sup> However, the opinion stated that courts have analyzed the idea in one of two ways.<sup>133</sup> Under the first approach, the ECPA's interstate commerce clause is held to require that the information logged actually

---

<sup>126</sup> See e.g., COLO. REV. STAT. § 24-34-402.5(1)(a) (2008) (codifying this exception and allowing termination for an outside activity if it “[R]elates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular group of employees, rather than to all employees of the employer.”).

<sup>127</sup> See e.g. Jackson Lewis, *Keylogging Employees' Computer Use Met with Judicial Wariness*, June 5, 2009, <http://www.jacksonlewis.com/legalupdates/article.cfm?aid=1747> [hereinafter *Keylogging*] (stating that “[t]ypically, [keystroke logging] is done secretly, so the person using the keyboard is unaware his activities are being monitored.”).

<sup>128</sup> See e.g., *Keylogging*, *supra* note 127 (discussing a recent ECPA challenge to an employer's keystroke logging program which was used to discover a personal e-mail password).

<sup>129</sup> *Brahmana v. Lembo*, No. C-09-00106, 2009 U.S. Dist. LEXIS 42800, at \*2-5 (N.D. Cal. May 20, 2009) (stating that the plaintiff claimed that he had neither given permission to obtain this password nor discussed this password with any other employees).

<sup>130</sup> *Brahmana*, *supra* note 11, at 8 (proceeding to the interstate commerce prong of the ECPA interception analysis).

<sup>131</sup> See e.g., *United States v. Ropp*, 347 F. Supp. 2d 831, 832 (C.D. Cal. 2004) (stating that the defendant-employer claimed that logged keystrokes were merely prepared when typed but not sent as required by the ECPA). See also *United States v. Scarfo*, 180 F. Supp. 2d 572, 582 (D. N.J. 2001) (holding that the key-logger device which logged non-transmitted communications by ignoring all communications transmitted by a modem did not intercept information under the ECPA).

<sup>132</sup> *Brahmana*, *supra* note 11, at 9 (stating that the “court does not need to resolve at this time [which of the two analyses] of ‘affecting interstate commerce’ is correct.”).

<sup>133</sup> *Brahmana*, *supra* note 11, at 7-9.

travel in interstate commerce.<sup>134</sup> This would be a rare occurrence - especially for information logged by a device or software program located within the computer itself. The second approach requires only that the intercepted information somehow affect interstate commerce while not necessarily traveling in interstate commerce.<sup>135</sup> With this in mind, employers should be very careful before implementing key-logging monitoring.

Backspace and delete button monitoring might be the most obscure form of monitoring discussed in this section - but it happens. This type of monitoring tracks the number of times each button is struck over a specific assignment or period of time. The idea is that the more employees strike these buttons, the less efficient these employees are. Finally, language tracking software is designed to scan employee communications in search of inappropriate language. This form of monitoring looks for keywords typical of harassment and bullying.

## J. PHYSICAL SEARCHES

It is important to note that the searches described in this article constitute those made by employers or their employees looking for policy violations (employment-related searches) as opposed to searches made by law enforcement authorities within private workplaces looking for violations of the law (law enforcement-related searches). Employment-related searches are one of the oldest forms of employee monitoring.<sup>136</sup> Through such searches, employers generally seek to monitor employees for illegal drug use, theft, or the possession of alcohol or weapons.<sup>137</sup> A lesser known form of physical searches is referred to as dumpster diving. Dumpster diving is a rather drastic form of employee monitoring. This occurs when employers physically search through employee's trash and recycling looking for information. Oftentimes employees merely discard documents without shredding them. This allows an employer, with access to employee offices, to re-create an accurate record of employee actions in the workplace.

---

<sup>134</sup> See e.g., *Ropp*, at 837-38 (holding that the key-logger involved in the case:

[C]onsists of the local computer's hardware -- the Central Processing Unit, hard drive and peripherals (including the keyboard) -- and one or more software programs including the computer's operating system . . . and either an e-mail or other communications program being used to compose messages. Although this system is connected to a larger system -- the network -- which affects interstate or foreign commerce, the transmission in issue did not involve that system. The network connection is irrelevant to the transmissions, which could have been made on a stand-alone computer that had no link at all to the internet or any other external network. Thus, although defendant engaged in a gross invasion of privacy by his installation of the [key-logger on the plaintiff's] computer, his conduct did not violate the Wiretap Act.).

<sup>135</sup> See e.g., *Potter v. Havlicek*, No. 3:06-cv-211, 2007 U.S. Dist. LEXIS 10677, at \*21-22 (S.D. Ohio 2007) (holding that the electronic communications that are intercepted need not travel in interstate commerce in order to "affect interstate commerce" as required by the ECPA ).

<sup>136</sup> See e.g., Mark Jeffery, *Information Technology and Worker Privacy: A Comparative Study: Part I: Introduction*, 23 COMP. LAB. L. & POL'Y J. 251, 260 (Winter 2002) (stating that "[b]efore the advent of computers, surveillance at work almost always involved a physical intrusion: a supervisor looking over the employees' shoulders (or, more recently, a microphone or camera being pointed at them); or a physical search of the employee's place of work or locker, of their private property (such as bags), or even of their person.").

<sup>137</sup> See e.g., *Workplace Searches*, WORKPLACE FAIRNESS, <http://www.workplacefairness.org/searches?agree=yes> (last visited Aug. 4, 2009) [hereinafter *Workplace Searches*].

The law allows employers to retain access to all areas of their workplace - even if they provide individual employees with personal offices and vehicles. Employers have the right to enter these offices and conduct searches almost at any time. The only places that remain off-limits are those where employees retain a “reasonable expectation of privacy.” Such an expectation is common in personal belongings stored in offices (i.e, purses or wallets) and potentially locked desk drawers. Some employers have chosen to physically search employee vehicles. Random searches - even if included in a policy - are frowned upon. Physical searches involving personal items such as briefcases/wallets/purses or of an employee’s body are likely an invasion of an employee’s reasonable expectation of privacy.

Likely the most famous workplace physical search case is *O’Connor v. Ortega*.<sup>138</sup> In *O’Connor* an employer-hospital conducted a thorough search of the office of its residency director - who was accused of various improprieties.<sup>139</sup> The office searched multiple times and the investigators went through the director’s desk, file cabinets.<sup>140</sup> The Supreme Court held that an employer does not need a warrant to conduct a physical office search and when such a search occurs in a place where employees have reasonable expectations of privacy then the search must be reasonable at its inception and in its scope.<sup>141</sup> A search will be justified at its inception when the employer “when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file.”<sup>142</sup> Second, a search will be reasonable in scope when “the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the misconduct.”<sup>143</sup> Courts have held that public employers can get remove employees’ reasonable expectations of privacy via a specific policy regarding physical searches. Finally, although the employer in *O’Connor* was a public employer - and thereby bound by the Fourth Amendment prohibition against unreasonable searches and seizures - the case has relevance to the private sector as well. Various states passed legislation granting private employees the same privacy protections as public employees. At the end of the day, however, employment-related search cases are very fact specific and difficult to categorize as precedent.<sup>144</sup>

## **K. SOCIAL-NETWORK & SEARCH ENGINE MONITORING**

Employers often hire private investigation firms to uncover information related to employee behavior. This practice has become more common today as previous employers are reluctant to give references about applicants. Employers also conduct their own private investigations by collecting personal information from governments and private sources, from profiles on social networking sites, from blogs, from Web discussions and from Google searches. Oftentimes employees hire outside investigators to assist.

---

<sup>138</sup> See 480 U.S. 709 (1987).

<sup>139</sup> See *id.* at 711-14.

<sup>140</sup> See *id.*

<sup>141</sup> See *id.* at 724-26.

<sup>142</sup> *Id.* at 726.

<sup>143</sup> *Id.* at 726 (internal citations omitted).

<sup>144</sup> See e.g., *Workplace Searches*, *supra* note 137 (stating that “[c]ases involving the violation of privacy rights through unreasonable [physical] searches are often extremely factual and tend to be decided on a case-by-case basis.”).

Finally, pretexting is assuming a false identity in order to obtain information from another party. Hewlett-Packard (HP) used this practice to determine the leaker of sensitive information from company board meetings.<sup>145</sup> Private investigators hired by HP posed as third parties in an attempt to gain access to board members and journalist phone records to discover the leak. In 2007, President Bush signed the Telephone Records and Privacy Protection Act (TRPPA).<sup>146</sup> The TRPPA makes it illegal to utilize fraudulent practices to persuade phone companies to hand over confidential phone records. Before this law, it was already illegal to utilize pretexting to obtain another person's financial records.

Social Networking and Search Engine monitoring is one of the most recent forms of employee monitoring. It is also one of the cheapest. All an employer needs is an Internet connection, a browser and basic knowledge of how such programs operate. Social-networking monitoring involves creating an account on a Web site such as Facebook or MySpace and then searching the name of the employee/applicant. A treasure trove of information may appear at the click of a mouse as these sites make it easy to upload incriminating pictures, post silly or discriminatory quotations and identify known associates (i.e., friends). Unless the user sets the privacy setting to "Friends Only," their profile is freely available to anyone who searches. In fact, employees are becoming more conscious of just how easy this form of monitoring has become. 29% of employees have become more conservative online because they fear that "employers can use anything and everything as an excuse to fire" them in a down economy.<sup>147</sup>

Search engine monitoring is just as simple as social-network monitoring. To conduct these searches, an employer merely requests the a search engine homepage (such as Google.com or Yahoo.com) and searches for the employee's/applicant's name. Within seconds (Google even keeps track of the time it takes to complete the search) potentially hundreds of links appear. Most of the time the person's name appears somewhere within the Web page targeted by the link. Employees need only sit back and discover a great deal of potentially embarrassing information. It is much more easier to find juicy information about an employee on social networking sites because that is one of their major points of existence. However, conducting a Google search has some advantages over a Facebook search. First, individual's cannot make their name private from search. Indeed, it is very difficult to force a search engine to remove even one link an individual considers inappropriate. Second, employees do not need as much instruction on how to conduct a search engine inquiry as they do to navigate MySpace for information. In the end, both social-networking and search engine inquiries are legal, efficient, inexpensive and powerful monitoring tools.

## **L. TELEPHONE, TEXT MESSAGE & VOICEMAIL MONITORING**

---

<sup>145</sup> See e.g., Brittany Petersen, *Employee Monitoring: It's Not Paranoia - You Really Are Being Watched*, P.C. MAGAZINE, May 26, 2008, <http://www.pcmag.com/article2/0,2817,2308369,00.asp> (stating that the "chairman of HP and half a dozen board members resigned or were fired as a result [of the pretexting], and the entire debacle shed new light on the possibilities of employee monitoring in the digital age.").

<sup>146</sup> 109 Pub. L. No. 476, 120 Stat. 3568 (Jan. 12, 2007).

<sup>147</sup> See e.g., *Social Networking*, *supra* note 119, at 12.

Telephone monitoring tracks the amount of time spent on calls, phone numbers dialed, breaks between receiving calls, etc. Employers are looking for theft of trade secrets and confidential information, violence between co-workers or an employee and a customer, sabotage and performance issues. Merely monitoring telephone calls likely does not create major legal problems. Federal law and most state laws allow monitoring as long as one party to the conversation consents. With this in mind, companies create telephone monitoring consent policies satisfying this requirement. For instance, Wal-Mart's monitoring policy states that "all electronic communications of associates using Wal-Mart communication systems are subject to monitoring and recording."<sup>148</sup> This policy would count as Wal-Mart consenting as one part to a telephone conversation. Recording employee telephone calls, on the other hand, would present problems. In fact, Wal-Mart recently terminated an employee for monitoring telephone conversations between a company public relations representative and a reporter for the New York Times.<sup>149</sup>

Voicemail monitoring allows employers to listen to employee voicemail in order to determine the same issues as are relevant in telephone monitoring. Contemporary voicemail programs can monitor messages using a "Unified Messaging" program that turns voicemail into audio files and e-mail text.. Finally, text messages are fast becoming the preferred method of communication. Text messages are composed and sent via cell phone to recipients from the user's contacts list. Employees are much more likely to monitor text messages sent from employer-provided equipment than from employee's personal cell phones.

## **M. VIDEO SURVEILLANCE**

Video surveillance involves the taping of employees within workplace facilities or outside of the workplace conducting work activities.<sup>150</sup> In lieu of software desktop, e-mail or Internet monitoring, employers can point a video camera directly at computer screens to monitor computer-based activity. In a 2007 survey by the American Management Association, 47% of employers admitted to monitoring their employees via this method - up from just over 30% in 2001.<sup>151</sup> Just under 50% of those admitting to monitoring claimed that video surveillance is ongoing as opposed to routine, occasional or specific.<sup>152</sup> Video surveillance is primarily intended to:

---

<sup>148</sup> See Caroline McCarthy, *Wal-Mart Fires System Technician Over Pretexting Debacle*, C-NET NEWS, Mar. 5, 2007, [http://news.cnet.com/8301-10784\\_3-6164404-7.html](http://news.cnet.com/8301-10784_3-6164404-7.html) [hereinafter *Wal-Mart*].

<sup>149</sup> See e.g., *Wal-Mart*, *supra* note 148.

<sup>150</sup> See e.g., Alexandra Fiore and Matthew Weinick, Note: *Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change*, 25 HOFSTRA LAB. & EMP. L.J. 525, 526-27 (Spring 2008) [hereinafter *Undignified in Defeat*] (discussing employees under video surveillance at a Wal-Mart Store where the company recently "installed a video camera in the employee unisex bathroom to catch a suspected thief . . . [where] [t]heft and unauthorized conduct by employees led to the installation of a video camera in the employee locker room at Johnson County Community College [and where] workers at a Kentucky distribution center discovered a video camera installed in the men's bathroom.") (internal citations omitted).

<sup>151</sup> See e.g., *2007 AMA Survey*, *supra* note 2, at 7-8 (stating that this method was used to counter "theft, violence, or sabotage").

<sup>152</sup> See *id.* at 8.

1. Increase safety of employees (by decreasing violence and threatening behavior and locating workplace risks<sup>153</sup>);
2. Discourage drug/alcohol use, theft or sabotage and otherwise protect employer property; and/  
or
3. Monitor employee productivity.<sup>154</sup>

Some employers place hidden cameras throughout the workplace while others are purposefully overt.<sup>155</sup> Hidden cameras provide the element of surprise and are likely to capture more accurate results. Overt cameras, on the other hand, are placed in public view to discourage bad behavior and to encourage productivity. Other employers place fake or deactivated cameras in the workplace to gain the advantage of overt surveillance without the cost of actual cameras.<sup>156</sup> Finally, it is important to remember that employer-owned video surveillance equipment can be misused by employees which may lead to sexual harassment or invasion of privacy lawsuits.<sup>157</sup> Over 70% of employers who conduct video surveillance notify their employees before hand.<sup>158</sup>

---

<sup>153</sup> See e.g., *Napreljac v. Hammons Hotels, Inc.*, 461 F. Supp. 2d 981 (S.D. Iowa 2006), *aff'd* 503 F.3d 800 (8th Cir. 2007) (utilizing an employer's surveillance video to help determine whether an employee was injured on the job in the manner the employee claimed to be injured).

<sup>154</sup> See e.g., Alice Osborn, *Respecting Employee Privacy Rights in the Workplace when using Video Surveillance*, VIDEO-SURVEILLANCE-GUIDE, Aug. 17, 2005, <http://www.video-surveillance-guide.com/employee-privacy-rights-in-the-workplace.htm>. Interestingly, no companies monitored all of their employees via video to analyze productivity. (showing that, while no company monitored all employees via video, only 7% of companies monitored selected groups of employees to analyze productivities). See also *Undignified in Defeat*, *supra* note 150, at 527 (stating that employers use video surveillance "to monitor productivity, and to protect property and workers' safety." and Parry Aftab, *The Privacy Lawyer: To Videotape or not to Videotape*, INFORMATION WEEK, Aug. 16, 2004, available at <http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=26806697> (stating that:

Most of employers' monitoring and surveillance is designed to curtail theft and drug and alcohol use, identify potential workplace risks, and measure and improve employee performance. It has been reported that three-quarters of all drug users admit to using drugs at work, and 60% of them admit to dealing drugs at work. Given these statistics, it's not surprising that 20% of the drug users reported drug-impairment-related accidents on the job. Employers and their insurers have to take some kind of action to control this situation, and more and more often, they're resorting to workplace monitoring and surveillance tactics.).

<sup>155</sup> Some employers place video surveillance equipment throughout the workplace. See generally, *Williams v. City of Tulsa*, 393 F. Supp. 2d 1124 (2005) (discussing accusations that the defendant company placed video cameras and microphones in various workplace locations including near the restroom, inside supervisors' offices, in shop areas and even inside a clock).

<sup>156</sup> See e.g., *Data Protection: Video Surveillance and Data Monitoring: The Basics*, CSO ONLINE, [http://www.csoonline.com/article/221735/Video\\_Surveillance\\_and\\_Data\\_Monitoring\\_The\\_Basics?page=3](http://www.csoonline.com/article/221735/Video_Surveillance_and_Data_Monitoring_The_Basics?page=3) [last visited July 23, 2009] [hereinafter *Data Protection*] (stating that "[f]ake or deactivated cameras are an attempt get the deterrence value of surveillance without incurring the expense of video storage and maintenance.").

<sup>157</sup> See e.g., *EEOC v. Smokin' Joe's Tobacco Shop*, No. 06-01758, 2007 WL 1258132, at 4 (E.D. Pa. 2007), available at <http://www.paed.uscourts.gov/documents/opinions/07D0529P.pdf>. (ruling on a hostile environment sexual harassment lawsuit where an employee "used the [employer's] video surveillance system to watch women [in the workplace], which made [the plaintiff] and other female employees [in the workplace] uncomfortable.").

<sup>158</sup> See e.g., *2007 AMA Survey*, *supra* note 2, at 8.

Video surveillance is relatively expensive in terms of bandwidth and storage requirements<sup>159</sup> - although such costs decrease as technology advances.<sup>160</sup> Video surveillance is allowed under the ECPA but adding audio would cause problems.<sup>161</sup> The only real remedy against video surveillance in private workplaces lies in tort law - more specifically in the torts of intrusion upon seclusion and intentional infliction of emotional distress<sup>162</sup> -and via scattered state laws.<sup>163</sup> More importantly, however any type of video surveillance is likely to decrease employee morale, increase stress, lead to distrust and decrease productivity.<sup>164</sup>

#### IV. A NEW & EFFECTIVE EMPLOYEE MONITORING FRAMEWORK

-- As many technologies speed past the law in general, the particular technologies enabling electronic monitoring in the workplace have outpaced the legislature's ability to react with a reasoned solution reflective of society's values. Likewise, the common law is so entrenched in legal precedent, which inadequately corresponds to the reality of the 'wired' worksite, that it has not been able to respond in a timely fashion either.<sup>165</sup> --

---

<sup>159</sup> See *Data Protection*, *supra* note 156 (fielding questions from employers regarding the costs of video surveillance such as “[a] big cost consideration is frame rate, which affects our tape requirements or storage and bandwidth requirements.”).

<sup>160</sup> See *e.g.*, *Undignified in Defeat*, *supra* note 150, at 525-26 (stating that, “while the sophistication of surveillance equipment is increasing, the cost is falling precipitously. ‘A decent closed-circuit TV [set up] costs less than \$ 3,000, and the cameras, using fiber-optic technology, can acquire a good image from a hole the size of a pencil point.’ A range of technology including hidden cameras, recording devices, and tiny wireless cameras, is available for less than five hundred dollars.”) (internal citations omitted).

<sup>161</sup> See *e.g.*, *United States v. Koyomejian*, 970 F.2d 536, 537 (9th Cir. 1992) (holding that silent video surveillance “is neither prohibited nor regulated by Title I” of the ECPA). Various state electronic communications laws have been interpreted to allow silent video monitoring. See *e.g.*, *Audenreid Circuit City Stores, Inc.*, 97 F. Supp. 2d 660, 663 (E.D. Pa. 2000) (holding that “[i]n the absence of any record of ‘a human voice at any point between and including the point of origin and the point of reception,’ as is required for an ‘aural transfer,’ we can reach no other conclusion but that the [ECPA] and Pennsylvania Wiretapping and Electronic Surveillance Control [Act] have no application here and that the defendant did not violate either of these acts in placing the video camera in Plaintiff’s office.”). This is true even if a video surveillance camera - without audio capabilities - is placed in an employee locker room. See *e.g.*, *Thompson v. Johnson County Community College*, 930 F. Supp. 501, 506 (D. Kan.), *aff’d* 108 F.3d 1388 (10th Cir. 1997) (finding that the “defendants installed a silent video surveillance camera in the security personnel locker area. Because the use of a silent video surveillance camera does not violate Title I [of the ECPA], the court concludes, as a matter of law, that defendants are entitled to summary judgment on this issue.”).

<sup>162</sup> See *e.g.*, *Undignified in Defeat*, *supra* note 150, at 527.

<sup>163</sup> See *e.g.*, CONN. GEN. STAT. § 31-48b(b) (2008) (stating that no “employer or agent or representative of an employer shall operate any electronic surveillance device or system, including but not limited to the recording of sound or voice or a closed circuit television system, or any combination thereof, for the purpose of recording or monitoring the activities of his employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, locker rooms or lounges.”) and N.Y. LAB. LAW § 203-c (McKinney 2008) (stating that no “employer may cause a video recording to be made of an employee in a restroom, locker room, or room designated by an employer for employees to change their clothes, unless authorized by court order [and] [n]o video recording made in violation of this section may be used by an employer for any purpose.”). Note that these statutes only prohibit video surveillance in very personal areas of the workplace and not in more public areas.

<sup>164</sup> See *e.g.*, *Undignified in Defeat*, *supra* note 150, at 530-31 (stating that uncertainty surrounding video surveillance “adds to workplace stress and violates a person's sense of dignity. An Australian Privacy Commissioner's study concluded that video surveillance substantially impacts the work environment. Video surveillance has the effect of undermining morale and creating distrust and suspicion between employees and management.”) (internal citations omitted). See also G. Stoney Alder, *Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives*, 17 J. BUS. ETHICS 729, 730-42 (1998) (arguing that employee electronic monitoring is not inherently ethical or unethical while also collecting major arguments for and against such monitoring from various ethical frameworks).

<sup>165</sup> Jay P. Kesan, *Cyber-Working or Cyber-Shirking? A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 304 (2002) [hereinafter *Cyber-Working*].

This section combines the patchwork regime analyzed in Part II and the powerful monitoring technology identified in Part III and proposes a framework. This framework provides guidance for employers to create or revise employee monitoring policies. This framework also provides structure for Congress to draft a desperately-needed employee monitoring regime.<sup>166</sup> Two components are necessary for an effective monitoring regime. First, private employers must be required to provide notice of any monitoring that may take place. A notice requirement is the low-hanging fruit, so to speak, in this area and should be easy for Congress to enact and for employers to implement. Notice by itself, however, is insufficient. Therefore, the remainder of the section discusses the second component necessary for an effective monitoring regime - the classification of each of the top monitoring practices into one of four categories. Each category takes into account employee privacy interests and an employer enterprise protection interests. The employee interests are considered by analyzing the degree to which each monitoring practice invades upon an employee's "reasonable expectation of privacy." The employer interests are considered by evaluating the benefits that the monitoring practice has on the three Monitoring Purposes identified in Part I:

1. The degree to which the monitoring aids employers in conducting and completing business transactions (Business Purpose);
2. The degree to which the monitoring aids employers in preventing civil lawsuits or criminal prosecutions (Liability-Avoidance Purpose); and
3. The degree to which the monitoring aids employers conducting a pending internal or external investigation (Investigatory Purpose).

Each of the four categories balances these interests on a high/low scale.<sup>167</sup> The first category includes monitoring practices that constitute low privacy invasions and provide high enterprise protection. These practices are the most valuable to the enterprise as a whole and are a fair compromise under the employment-at-will relationship. This category is styled **BEST PRACTICES**. The second category includes monitoring practices that constitute high privacy invasions but also provide high enterprise protection. This classification is a grey area in the employee monitoring arena and can lead to serious privacy invasions unless implemented and audited carefully. This category is styled **RISKY PRACTICES**. The third category includes monitoring practices that constitute low privacy invasions but also provide low enterprise protection. These monitoring techniques do not add much to an employer's overall understanding of employee activities and may not be worth the decrease in morale and trust that accompanies them. This category is styled **BORDERLINE PRACTICES**. Finally, the fourth category includes monitoring practices that constitute a high privacy invasions while providing low enterprise protection. Employers implementing the monitoring practices in category four are likely to experience a decrease in morale and a high turnover rate - especially considering the notice of monitoring requirement that must be enacted. To eliminate any incentive employers might find to conduct these practices, the law should broadly prohibit them in the workplace. This category is styled **POOR**

---

<sup>166</sup> Any new employee monitoring regime is more appropriately passed by Congress as opposed to various state legislatures. A nationwide legal structure would benefit both employees (who often change jobs interstate) and employers (who would crave a standardized approach as opposed to at least fifty different compliance obligations).

<sup>167</sup> It would certainly be possible to make a more in-depth analysis of each practice. However, the binary, high/low analysis utilized in this section serves the overarching framework proposed in this article. Interestingly most of the top monitoring practices easily fall into the high or low protection/benefit classification.

**PRACTICES.** The remainder of this section evaluates which monitoring practice best fits in each category and ends with a visual description of the results.

## **A. THE LOW-HANGING FRUIT: THE LAW MUST REQUIRE NOTICE OF MONITORING PRACTICES**

A legal requirement that employers provide notice of their monitoring practices is a no-brainer. In fact, the vast majority of employers already give notice.<sup>168</sup> While the issue of requiring notice has been fully addressed in the academic literature,<sup>169</sup> it is important to reiterate the strong reasons for implementing a notice requirement. First, providing notice to employees is a simple and inexpensive process - especially if provided electronically via e-mail or on a company's Intranet.<sup>170</sup> Second, notice requires employers to carefully analyze their monitoring practices - an exercise that, in itself, can help reduce legal liability as employee interests are considered more thoroughly. Finally, employees receiving notice will: (1) be wary (hopefully!) of conducting illegal or unethical activities while at work,<sup>171</sup> (2) understand that any personal tasks they choose to undertake at work may be monitored and (3) be able to

---

<sup>168</sup> See e.g., Nathan Watson, Note: *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?*, 54 FED. COMM. L.J. 79, 100 (2001) [hereinafter *The Private Workplace*] (stating that "a notice requirement will not burden employers. In fact, most employers who engage in the practice of electronic monitoring do give notice. This may be due to lawyers advising employers to give notice in order to fight off potential state invasion of privacy suits; as with notice, there is no reasonable expectation of privacy. Whatever the motivation, that such practices are developed at all shows that employers do not unduly suffer from having to give notice of electronic monitoring.") (internal citations omitted) and *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987 and H.R. 4908 Before the House Subcomm. on the Const. of the Comm. on the Judiciary*, 106th Cong. 197 (2000) (statement of Lewis Maltby, President, National WorkRights Institute).

<sup>169</sup> See generally, Mindy C. Calist, Note, *You are Being Watched: The Need for Notice in Employer Electronic Monitoring*, 96 KY. L.J. 649, 667-68 (2007-2008) [hereinafter *You are Being Watched*] (arguing for a comprehensive regime requiring notice of employee monitoring); William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOKLYN L. REV. 91, 115-117 (Fall 2003); Charles E. Frayer, Note: *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity With Legitimate Management Interests*, 57 BUS. LAW. 857 (2002); Jay P. Kesan, *Cyber-Working or Cyber-Shirking? A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 305 (2002); Amanda Richman, Note, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337, 1358-61 (2001) (arguing for the adoption of a federal monitoring notice bill such as the Privacy for Consumers and Workers Act (PCWA)); *The Private Workplace*, supra note 168, at 99-102 (arguing for the Notice of Employee Monitoring Act); and S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 849-53 & 879-87 (1998) (discussing failed federal notice bills and arguing for comprehensive privacy protection in the workplace).

<sup>170</sup> See e.g., *The Private Workplace*, supra note 168, at 99 (stating that a "rule addressing electronic monitoring should have a notice requirement for several reasons. First, notice should be given to employees because it is simply the right thing to do. Second, a notice requirement is a simple and cheap solution to this problem. Third, a notice requirement will deter employees from engaging in activity that could be harmful or offensive to others, such as sexual harassment through e-mail. Finally, a notice requirement will give employees needed information to decide if they wish to continue working for the employer.")

<sup>171</sup> Also, "a notice requirement will deter employees from engaging in activities that may lead to liability for the employer. Because employers can be held liable for their employees' actions, conduct such as sexual harassment through e-mail or the downloading of offensive pictures from the Internet can lead to legal trouble for employers. An employee who knows he is being monitored will probably not engage in such activity." *Id.* at 100. See also *You are Being Watched*, supra note 169, at 659-60 (stating that providing notice of monitoring practices "can establish the [personal] activity deemed inappropriate, and will give employees a better understanding of the conduct that would violate the employment policies.").

analyze a company's monitoring practices and decide whether they desire to continue their current employment or desire to organize to change the policy.<sup>172</sup>

At the same time, notice allows employers to: (1) clearly articulate their monitoring policies and minimize misunderstanding, (2) craft and distribute policies that allow for some personal tasks to be undertaken on work time,<sup>173</sup> (3) decrease an employee's reasonable expectation of privacy<sup>174</sup> and (4) document that they have attempted to mitigate against unlawful employee activities.<sup>175</sup> Employers are also less likely to violate a policy that has been distributed to all employees.<sup>176</sup> An effective monitoring regime must require employers to provide notice that:

1. Is written in plain English;<sup>177</sup>
2. Is issued in writing or posted electronically in advance of any monitoring;
3. Is provided to all current employees and all new hires prior to their first paid day of work,
4. Is reissued every year and immediately upon any amendment;
5. Requires employees to acknowledge receipt;

---

<sup>172</sup> See e.g., *The Private Workplace*, supra note 168, at 99-100 (stating that “[s]ince employers cannot reasonably expect employees in today's world to abstain from handling personal matters in the workplace, employees should at least be given warning that employers are watching. If employees desire absolute privacy, they will know that they will not be able to obtain it through their employers' computer systems.”).

<sup>173</sup> Notice provides the opportunity for employers to state what is acceptable and for employees to give employers feedback regarding what should be acceptable. Therefore, a reasonable policy can be established that will allow employees “to use the Internet for personal matters before or after normal work hours and/or during their lunch hours.” *Id.* at 100.

<sup>174</sup> See e.g., *You are Being Watched*, supra note 169, at 659 (stating that “[n]otice significantly decreases the employee's reasonable expectation of privacy, and thus helps further insulate the employer from liability.”).

<sup>175</sup> See e.g., *The Private Workplace*, supra note 168, at 100 (stating that “notice can provide an opportunity for employers to make clear that ‘use of the [employer's technology] in a manner that might create a hostile work environment on the basis of race, sex, age or other protected classifications should be expressly prohibited.’”).

<sup>176</sup> See e.g., *You are Being Watched*, supra note 169, at 659-60 (stating that notice “can additionally have a deterrence effect - it might deter some employers from engaging in unlawful monitoring, and it would certainly deter many employees from engaging in conduct that could be grounds for termination.”).

<sup>177</sup> See e.g., Corey Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 14 (2009) (discussing a plain English requirement for Web site privacy policies and stating that:

Borrowed from the realm of securities regulation, Plain English is a concept designed to eliminate writing styles and phrasing that the average citizen struggles to understand. This is important in a country where hundreds of millions of people (approximately 72% of the United States population) from all different ages and educational/technological backgrounds have Internet access. A Plain English document “uses words economically and at a level the audience can understand. Its sentence structure is tight. Its tone is welcoming and direct. Its design is visually appealing. A plain English document is easy to read and looks like it's meant to be read.” Plain English documents should avoid:

- Long sentences;
- Passive voice;
- Weak verbs;
- Superfluous words;
- Legal and financial jargon;
- Numerous defined terms;
- Abstract words;
- Unnecessary details; and
- Unreadable design and layout.

(internal citations omitted). See also Securities & Exchange Commission, *A Plain English Handbook: How To Create Clear SEC Disclosure Documents* (Aug. 1998), available at <http://www.sec.gov/pdf/handbook.pdf>.

6. Contains information on the types of monitoring conducted, the types of information obtained, the reasons for the monitoring, the frequency of the monitoring, how the information may be used and how long the information will be retained;
7. States where employees may report violations of the monitoring policy and make suggestions as to how the policy may be improved.

However appealing a mandatory-notice regime appears upon first glance, its effectiveness can be misleading. For example, mandatory notice is a bit illusory as employers are allowed to monitor as they please as long as they accurately disclose such practices.<sup>178</sup> Employees might tolerate excessive monitoring instead of leaving their employer - especially in an economy with high unemployment and underemployment rates. Therefore, notice must merely comprise the first component of a more robust monitoring regime which includes substantive restrictions on monitoring. This remainder of this section argues that additional restrictions be mandatory for all private sector employers and be based on the four categories below. Under such a monitoring regime, employers should have to provide notice AND should be prohibited from conducting monitoring outside of the allowable business purpose identified in each category.

## **B. CATEGORY ONE: BEST PRACTICES**

An effective monitoring regime must allow, and even encourage, employers to implement best practices. Best practices are “fundamental principles that add value to organizational performance [and] workplace behavioral standards that contribute to consistently excellent performance by employees and teams of employees.”<sup>179</sup> Wise managers strive to identify and implement best practices into their policies and operations - both internally and externally. Best practices are crucial when it comes to sophisticated monitoring technology and its potential to invade employee privacy. The creation of best practices forces employers to analyze the following issues:

- (1) Is the proposed monitoring necessary under any of the three key Monitoring Purposes?;
- (2) Which types of monitoring is most appropriate for which Monitoring Purpose?;
- (3) How might the monitoring be abused/thwarted by rogue or unhappy employees/supervisors?;
- (4) How can management clearly explain the monitoring practices via the required notice?; and
- (5) How might management's failure to carry out the monitoring policy lead to legal liability?

Theoretically, understanding the importance of best practices and asking these five questions would be enough for management to draft, execute and adhere to an effective and fair monitoring policy. Realistically, while many businesses care about these issues and take employee monitoring seriously, others do not give a second thought to employee morale and ongoing privacy invasions. Although the law cannot force management to diligently consider their monitoring scheme or care about employee morale, it can create baseline standards. Therefore, an effective monitoring regime identifies which forms of monitoring constitute best practices and allow employers to implement such practices for all three Monitoring Purposes. Monitoring that falls outside of these three purposes - i.e., a case where an

---

<sup>178</sup> See e.g., *Cyber-Working*, *supra* note 7, at 305 (stating that “[w]ith notice, employees are still exposed to electronic monitoring with very few limitations.”).

<sup>179</sup> Securiguard, *Security Services Glossary*, available at <http://www.securiguard.com/glossary.html> (last visited May 2, 2010).

employee taps into a subordinate's attendance records and issues a complaint to satisfy a personal grudge - must be prohibited. The following three of the top monitoring practices into the Best Practices category:

1. Access Panels;
2. Attendance & Time Monitoring; and
3. Automatic Screen Warnings

## **ACCESS PANELS**

Access panels are relatively harmless. These devices cannot sift through personal e-mails or listen in on private phone calls. The job of an access panel is to collect information on comings and goings and allow/disallow access. A new monitoring regime should allow the installation of access panels on all outside access doors and other important and/or secure areas. These panels must be allowed to record who enters the area and at what time, who exists the area and at what time and be able to log the total time spent inside. This information should be readily accessible for all three Monitoring Purposes - especially in the event of an emergency or as part of an employee's periodic review, discipline or termination decision. Obviously, companies can abuse access panels to the point where their use no longer constitutes a best practice. For example, placing access panels on restroom or locker room doors is overkill and can morph this form of monitoring into the high privacy invasion variety.<sup>180</sup> A new monitoring regime should prohibit access panels from logging any information on use of private places. If an employer desires to keep a private area secure or monitor ingress and egress - management can use an ancient lock and key system or station personnel at such locations. At the end of the day, access panels are not very invasive to employee privacy and can legitimately protect an enterprise. Therefore, a new monitoring regime should broadly allow access panel monitoring for all three Monitoring Purposes.

## **ATTENDANCE & TIME MONITORING**

Another best practice is for employers to keep track of employee attendance. The detail of such logs varies between industries. Some employers, such as law firms, need only insure that employees are completing tasks. Other employers, such as educational institutions, need to monitor a teacher's daily attendance. Finally, some employers, such as retailers, need to monitor employees by the hour. Attendance monitoring is especially important when the employment relationship sours. Oftentimes, employees argue that their terminations are against public policy because their poor attendance stems

---

<sup>180</sup> Under the new monitoring framework, for example, management at a Ford plant in Wayne, Michigan could not monitor employee bathroom use via an access panel. See e.g., *Ford Eyeing Bathroom Breaks*, CNN/MONEY, Oct. 27, 2005, [http://money.cnn.com/2005/10/27/news/fortune500/ford\\_bathroom\\_breaks/](http://money.cnn.com/2005/10/27/news/fortune500/ford_bathroom_breaks/) (stating that "management at the company's Michigan Truck plant . . . issued a memo in which it said too many of the factory's 3,500 hourly workers are spending more than the 48 minutes allotted per shift to use the bathroom. The extra-long breaks are slowing production of the Ford Expedition and Lincoln Navigator sport utility vehicles"). This new monitoring regime would not prevent Ford from monitoring restroom abuses in the absence of sophisticated monitoring technology - although such a practice would likely be bad for morale as well.

from medical or family issues.<sup>181</sup> These employees then seek unemployment benefits which are denied because their terminations are for just cause.<sup>182</sup> Courts then look to company attendance policies and attendance logs to make a ruling.<sup>183</sup> Without attendance monitoring in effect, employees who shirk and miss work for non-legitimate reasons have a much easier time claiming undeserved benefits and perhaps succeeding in wrongful termination lawsuits. Detailed attendance monitoring systems also allow employers to take into account situations where employees legitimately miss work for legitimate reasons and work with individuals to find a solution. Attendance monitoring constitutes a low invasion of employee privacy and can protect the enterprise in many legitimate ways. Therefore, a new monitoring regime should broadly allow attendance and time monitoring for all three Monitoring Purposes.

## **AUTOMATIC SCREEN WARNINGS**

Automatic screen warnings are a simple form of notice that can go a long way in educating and reminding employees about company monitoring policies. Although some employees might be frustrated that they have to click through the warning screen at first, in the long run, it will soon become routine. Management is best served by drafting the warning screens in such a way that employees buy in to the monitoring. As described in Part III, most forms of automatic warnings are drafted in legalese and meant to frighten employees into compliance. A better message would be something drafted in plain English to the effect of: “We value your intuition in making personal choices on work time. Please be conscious of our monitoring policy and understand that we may monitor your e-mail and Internet use. For the full monitoring policy, [click here](#).” Such warnings constitute low invasions of employee privacy and can protect an enterprise from liability by defeating an employee’s reasonable expectation of privacy. Therefore, a new monitoring regime should allow employers to utilize automatic screen warnings for all three Monitoring Purposes.

## **C. CATEGORY TWO: RISKY PRACTICES**

At some point, companies large and small will consider implementing each of the monitoring practices classified in Category Two.<sup>184</sup> However, unlike the best practices detailed in Category One, this type of

---

<sup>181</sup> See e.g., *Heckey v. Standard Motor Products, Inc.*, 708 P.2d 1003, at 2-3 (Kan. Ct. App. 1985) (unpublished opinion) (holding that a company was allowed, under the doctrine employment-at-will, to terminate an employee for violating its attendance standards). The company had kept detailed attendance records to support its case. *Id.* at 2.

<sup>182</sup> See e.g., *Johnson & Hardin Co. v. Admr., Ohio Bureau of Emp. Services*, 1989 LEXIS 2535, \*2-5 (Ohio Ct. App. June 28, 1989) (discussing a case where an employee was terminated for nine unexcused absences and later sued claiming that the termination was without just cause as required to receive unemployment benefits.).

<sup>183</sup> *Id.* at 2 (stating that a printing business “chose to establish what has been referred to as a ‘no-fault’ employee attendance monitoring and progressive discipline policy, apparently because of the deadline pressures of its industry. Under its policy, instances of [plaintiff employee’s] tardiness, early departure or absenteeism . . . were accumulated over a twelve-month period. As the number of [plaintiff employee’s] occurrences exceeded stated thresholds, a three-step disciplinary procedure of written warnings and suspension without pay was followed. Ultimately, after nine occurrences had been accumulated, [plaintiff employee] was discharged.”).

<sup>184</sup> *2007 AMA Survey*, *supra* note 2, at 1 (finding that employers are “primarily concerned about inappropriate Web surfing, with 66% monitoring Internet connections. Fully 65% of companies use software to block connections to inappropriate Websites—a 27% increase since 2001 when AMA/ePolicy Institute first surveyed electronic monitoring and surveillance policies and procedures.”). 45% of employers claimed that their either monitored social networking Web sites or did not know whether they monitored such Web sites. See *id.* at 6.

monitoring is riskier. Whereas best practices have a low impact on employee privacy and morale, risky practices are more invasive and can negatively impact an employee's perception of the workplace. Armed with this information, a new legal regime should broadly allow this type of monitoring only for Liability-Prevention and Investigatory Purposes. When utilized for Business Purposes, these risky monitoring practices should be restricted to cases where an employer passes the Privacy Judgment Rule (PJR). The PJR requires that: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Business Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). Employers should be given some leeway when they make good faith mistakes operating under the PJR. However, the law should punish employers who act outside of its prohibitions - in this case, when management uses risky monitoring practices for Business Purposes outside of the PJR.<sup>185</sup>

For example, it is excessively invasive for an employer to monitor social networking Web sites to determine if employees spent their weekend at the office as per management's request. These inquiries are clearly not "necessary for the specific Business Purpose (tracking employee attendance) involved" and are best made outside of the lens of powerful monitoring technology. Additionally, this type of monitoring is not narrowly tailored as employers will be able to learn much more about their employees from Facebook than merely where they spent the weekend. This specific monitoring exercise would violate the PJR. Even using risky monitoring practices for Liability-Avoidance Purposes is questionable considering the intrusiveness and paternalism that Internet monitoring, for example, engenders. However, the framework sketched in this article is not meant to encourage lawmakers to micromanage employers and their monitoring preferences. The monitoring practices in Category Two are merely risky and not invasive enough to prohibit for Liability-Avoidance and Investigatory Purposes. With these criteria in mind, the following three of the top monitoring practices fall into Category Two:

1. Filters & Firewalls;
2. Internet & Clickstream Data Monitoring; and
3. Social Networking & Search Engine Monitoring

## **FILTERS & FIREWALLS**

---

<sup>185</sup> Congress will need to determine the proper penalties for violations in consultation with industry and privacy groups. It would seem that a three strike system of warnings - at least for the risky practices in Category Two - is appropriate. After strike three, an escalating fine structure could be imposed. A comprehensive database or Web site where employees could report violations would help the relevant governmental agency - likely the Federal Trade Commission - to recognize and remediate violations.

Management may create filters/firewalls which block access to Web sites unrelated to employee job descriptions.<sup>186</sup> In fact, sixty-five percent of companies implement some form of filtering - generally blocking out pornographic, gaming and social networking Web sites.<sup>187</sup> While this technology is very effective at blocking access to suspicious/malicious sites, such restrictions do not enhance employee morale.<sup>188</sup> For example, denying employees access to Hotmail accounts, The Weather Channel or the local news Web site is seen as paternalistic.<sup>189</sup> There is little wrong with an employee spending ten minutes over lunch or on a break checking baseball scores on ESPN.com. In addition, it is nearly impossible to block all suspicious/malicious Web sites and permit the thousands of Web sites that might increase employee productivity. Finally, the benefits gained via filters and firewalls may not be worth the negative gossip generated around the old-fashioned water cooler.

As proposed in the introduction to this section, filters and firewalls should be restricted when utilized for Business Purposes to cases where: (1) the employer acts upon a reasonable business judgment that the filter/firewall is necessary for the specific Business Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). At the end of the day, employers should choose wisely before opting for incorporating filters and firewalls into their network to insure that they meet the PJR.

## **INTERNET & CLICKSTREAM DATA MONITORING**

As detailed in Part III, contemporary technology allows managers to monitor every step of an employee's online footprint. Sixty-six percent of companies take advantage of this sophisticated technology and choose to monitor the Internet activities of their employees.<sup>190</sup> Employers who chose to monitor in this way might discover that their employees are committing crimes or viewing pornography online. In such cases, employers can discipline or terminate the offender quickly and increase their

---

<sup>186</sup> Recall from Part III that a firewall is:

A piece of "computer hardware or software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outsider computer users (as of the Internet)." It can also be "programmed to analyze the network traffic flowing between [a] computer and the Internet"; it then "compares the information it monitors with a set of rules in its database," and "[i]f it sees something not allowed . . . the firewall can block and prevent the action." Further, [most] "firewall programs let you adjust the rules to allow certain types of data to flow freely back and forth without interference.

*U.S. v. Ziegler*, 474 F.3d 1184, 1186 (9th Cir. 2007) [hereinafter *Ziegler*] (internal citations omitted). Filters are similar and, therefore, will be encompassed in the firewall label for the remainder of this section.

<sup>187</sup> See e.g., *2007 AMA Survey*, *supra* note 2, at 5-6.

<sup>188</sup> Disallowing access to Web sites on work time can reduce liability as employees cannot download pornography without access to pornographic Web sites. However, there are multiple Web sites that provide directions allowing employees to circumvent a company's filter/firewall. See e.g., *How To Bypass a Firewall or Internet Filter*, WIKIHOW.COM, <http://www.wikihow.com/Bypass-a-Firewall-or-Internet-Filter> (last visited May 23, 2010).

<sup>189</sup> In fact, an employer should hope that its employees are savvy enough to find a way to access these banned sites over their PDA or personal laptop wifi connection.

<sup>190</sup> See e.g., *2007 AMA Survey*, *supra* note 2, at 5.

chances of fending off vicarious liability.<sup>191</sup> More likely, however, employers merely risk discovering that a vast majority of their employees spend time on benign Web sites unrelated to work. This puts employers in a bind as many hard working, productive employees often conduct personal tasks during their long workday. In addition, employees resent the idea that management monitors their online activities. Some employees have even quit based on the practice and the unequal enforcement of Internet monitoring policies.<sup>192</sup>

Courts generally uphold an employer's right to conduct Internet monitoring because employees cannot develop a reasonable expectation of privacy in the Web sites they visit at work.<sup>193</sup> This precedent is a fair compromise of employee/employer interests because the employer provides the network access and oftentimes the equipment and must protect itself from liability. One privacy expert made a similar claim, discussing the viewing/downloading of discriminatory pictures in the workplace, in this manner:

An employer should not have to tolerate use of its equipment for illegal purposes or risk responsibility for its employees' illegal conduct. Employers might also reasonably prohibit computer use that would be unlawful, such as a defamatory communication. Employers might [for example] reasonably prohibit images of a racial or sexual nature that might offend co-workers. While there is far-ranging debate on the appropriateness of restricting people's right to free speech in order to promote the equality of women and racial minorities, it is well-established within the workplace that certain speech and conduct must be prohibited or else racial or sexual harassment might result. Prohibiting this category of racial or sexual images protects employers from liability. . . . And for purposes of a workable privacy policy, it is reasonable to permit employers to prohibit the entire category of images when appropriate safeguards to protect employees' privacy are in place. Racist statements and sexual pictures that are, inadvertently or purposefully, exposed to co-workers do have the potential to offend co-workers. Such images can also contribute to a workplace that is inhospitable to women or minorities, despite not rising to the level of legally "hostile." Additionally, society generally disapproves of these types of materials at work. Moreover, it is likely easier and less expensive to monitor for all types of sexual and racial images rather than having to develop a monitoring system that aims to monitor only those that amount to unlawful sexual or racial harassment.<sup>194</sup>

---

<sup>191</sup> See e.g., *Doe v. XYZ Corp*, 887 A.2d 1156, 1169-70 (N.J. App. 2005) [hereinafter *Doe*] (holding that an employer might avoid vicariously liability when one of its employees transmits child pornography at work and the employer had policies against such activities). In the *Doe* case, however, the employer knew of the illegal activities and did little to nothing to shut them down or discipline the employee. *Id.* at 1169. The appellate court remanded the case for a jury trial but likely would have dismissed the employer from the case had management enforced its Internet policy. *Id.* at 1169-70.

<sup>192</sup> See e.g., *Safo v. Prof'l Warehouse*, 2008 Minn. App. Unpub. LEXIS 728, at \*5-6 (Minn. Ct. App. 2008) (unpublished opinion) (discussing an employee who sought unemployment benefits based, in part, because "she quit for good reason because of the employer's Internet policy, which restricts employees from using the Internet for personal reasons."). The employee claimed that the policy was reasonable but that "other employees used the Internet for personal reasons with impunity." *Id.* at \*6.

<sup>193</sup> See e.g., *Doe*, *supra* note 191, at 1167 (upholding an employer's Internet monitoring policy, questioning whether, "with actual or imputed knowledge that Employee was viewing child pornography on his computer, was defendant under a duty to act, either by terminating Employee or reporting his activities to law enforcement authorities, or both? [and concluding that such a duty exists]"). Employees may develop a reasonable expectation of privacy, however, if their online contact involves their attorney. See e.g., *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 663 (N.J. 2010) (holding that an employee who contacted her attorney over her employer's network and on her employer-provided laptop "had a reasonable expectation of privacy in the e-mails she exchanged with her attorney"). The *Stengart* case came about when, "in anticipation of discovery, Loving Care hired experts to create a forensic image of the laptop's hard drive, including temporary Internet files. Those files contained the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account." *Id.* at 655.

<sup>194</sup> Ariana R. Levison, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J. L. & PUB. POL'Y 609, 662-64 (summer 2009) [hereinafter *Industrial Justice*] (internal citations omitted).

This explains why, as with filters and firewalls, Internet monitoring should be broadly allowed for Liability-Prevention and Investigatory Purposes. Employers should be able to discover whether employees are viewing/downloading pornography or gambling on sports at work. However, Internet monitoring should be restricted when utilized for Business Purposes to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Business Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). Internet monitoring is a risky practice because it offers a moderate, albeit rather incomplete, method of enterprise protection and it is moderately invasive (though not nearly as invasive as monitoring an employee's e-mail account or physical location). Employers must be sure to meet the PJR in all cases of Internet monitoring for Business Purposes.

## **SOCIAL NETWORK & SEARCH ENGINE MONITORING**

Examining an individual's Facebook profile or Google dossier should be an important part of the hiring process.<sup>195</sup> Pre-employment is the best time to locate a picture of an excessively intoxicated applicant or a news story showing that an applicant stole money from a prior employer. This information is public, easy to locate and its posting speaks volumes about the applicant's character. Once an applicant has been hired, however, this type of investigation becomes more awkward and privacy invasive. Although the same information is available to employees both pre- and post-hiring, the terms of the relationship have changed dramatically. Employee morale takes a huge hit when employers pry into personal lives and activities of their employees - areas that generally have little to do with work. Additionally, this type of monitoring will rarely assist management for Liability-Prevention or Investigatory Purposes. It would be rare indeed for an employee to post pornographic pictures downloaded from work or comment about items stolen from the office. More commonly, employers monitor these Web sites looking for derogatory information posted about the company or merely to snoop on employees. The following are three telling examples:

- Thirteen Virgin Atlantic Airlines cabin crew members were fired after sharing their candid impressions of their employer, Virgin's planes and even passengers in a Facebook group. According to a Virgin Atlantic representative, "There is a time and place for Facebook. But there is no justification for it to be used as a sounding board for staff of any company to criticize the very passengers who ultimately pay their salaries."
- In June 2006, Marion County, Fla., Sheriff's Deputy Brian Quinn was fired for "conduct unbecoming an officer" after discovery of information on Quinn's MySpace page. Among other things, Quinn had posted a picture of himself in uniform, along with comments about women's breasts, binge drinking and nude swimming.
- On Oct. 31, 2007, Kevin Colvin told his employers at Boston's Anglo Irish Bank that he had to miss a day of work due to an emergency at home in New York. The next day, Colvin's manager happened to check the employee's Facebook profile, where Colvin had thoughtfully

---

<sup>195</sup> Recall that social network and search engine monitoring is not the monitoring of employee use of such Web sites at work. That type of monitoring would fall under Internet monitoring. Rather, this type of social network and search engine monitoring involves browsing through an employee's Facebook or MySpace page, etc. or conducting a Google search of an employee's name to discover information.

posted a photograph from a Halloween party he had attended the previous night, featuring him in a sparkly green fairy costume, complete with wand and a can of beer. Colvin's manager replied to an e-mail from his soon-to-be ex-employee, attaching the photo of Colvin in drag — and blind copying the entire office — and stating “Thanks for letting us know — hope everything is okay in New York (cool wand).” Colvin was fired for lying.<sup>196</sup>

As these three cases clearly demonstrate, social network monitoring is a cheap and effective way to discover personal information and track employee activities. The problem for employers lies in the fact that few of the issues mentioned above pertain in any detail to the jobs in question. In the first case, the employees were expressing an opinion outside of the workplace. In the second case, the employee was guilty of stupidity and immaturity - traits that the department surely could have discovered in a less invasive manner. Finally, in the third case, Mr. Colvin did lie and deserved a measure of discipline. Through its search, however, his employer may now face a lifestyle discrimination lawsuit.<sup>197</sup> This final point raises important issues; employees who suffer an adverse employment action based on social network or search engine monitoring may have a case against their employer under Title VII of the Civil

---

<sup>196</sup> John Browning, *Employers Face Pros, Cons With Monitoring Social Networking*, HOUSTON BUS. J., Feb. 27, 2009, available at <http://www.bizjournals.com/houston/stories/2009/03/02/smallb3.html> [hereinafter *Monitoring Social Networking*].

<sup>197</sup> See e.g., American Civil Liberties Union, *Legislative Briefing Kit: Lifestyle Discrimination in the Workplace*, [http://www.aclu.org/racial-justice\\_womens-rights/legislative-briefing-kit-lifestyle-discrimination-workplace#current](http://www.aclu.org/racial-justice_womens-rights/legislative-briefing-kit-lifestyle-discrimination-workplace#current) [hereinafter *Legislative Briefing Kit*] (last visited May 24, 2010) (posting a list of state lifestyle discrimination statutes).

Rights Act of 1964,<sup>198</sup> the Americans with Disabilities Act,<sup>199</sup> the Age Discrimination in Employment Act<sup>200</sup> or various state lifestyle discrimination laws.<sup>201</sup>

A new legal regime should allow this monitoring for Liability-Avoidance and Investigatory Purposes (i.e., an employer seeking information about an employee's character or integrity during a theft investigation). However, the invasiveness becomes excessive when employers use the same public information to make decisions about promotions or raises or merely to check in employee after-hours activities. Therefore, social network and search engine monitoring should be restricted when utilized for Business Purposes to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Business Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). Employers will always remain free to scour public sources of information like Facebook looking for information about employees. A new monitoring regime should, however, prohibit the use of such information against an employee unless management can meet the PJR test.

---

<sup>198</sup> 42 U.S.C. § 2000e-2(a)(1)-(2) (stating that it shall be an unlawful employment practice for an employer:

1. to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin; or
2. to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's race, color, religion, sex, or national origin.)

<sup>199</sup> 42 U.S.C. § 12112(a) (stating that "[n]o covered entity shall discriminate against a qualified individual on the basis of disability in regard to job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment.").

<sup>200</sup> 29 U.S.C. § 623(a) (stating that it shall be unlawful for an employer:

1. to fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's age;
2. to limit, segregate, or classify his employees in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's age; or
3. to reduce the wage rate of any employee in order to comply with this chapter.").

<sup>201</sup> *Id.* (stating that:

Let's say that you fire an employee . . . for lying, for discussing a company's trade secrets online, or for some other legitimate reason. If the worker's social networking profile contains personal information that identifies him or her as being in a protected class — such as age, ethnicity, race, gender or sexual orientation — a terminated employee can argue that the employer's snooping on Facebook made them aware of the employee's protected status. Without knowledge of a person's membership in a protected category, an employer can't be liable for discriminating on that basis. Add proof that the employer had such information through checking out a social networking site, however, and that defense becomes much more difficult for a company to maintain. Had [an employee] claimed he was fired based on a presumption about his sexual orientation, he might have had some basis under Massachusetts' fair employment practices law. When employees blog about living with a disability, or post photographs in which they can be clearly identified as ethnic minorities, an employer who monitors such sites runs the litigation risk of "too much information." They can also run afoul of states like New York that have "lifestyle-discrimination" laws — statutes that ban employers from considering off-duty conduct when making an adverse employment decision.)

*See also, Legislative Briefing Kit, supra* note 197 (identifying various state lifestyle discrimination laws that might pertain to this situation).

## D. CATEGORY THREE: BORDERLINE PRACTICES

The monitoring practices in Category Three are classified as borderline - each is highly effective and each is extremely invasive. More specifically, borderline practices such as e-mail monitoring and GPS tracking allow employers to quickly and accurately monitor the actions, communications and whereabouts of their employees. However, employee awareness of these increasingly-sophisticated practices increases stress, negatively impacts morale, lowers productivity and decreases employee willingness to use company equipment even for work purposes. Therefore, a new monitoring regime should balance the interests by permitting the use of borderline monitoring practices for all three Monitoring Purposes. However, while practices in the risky category were broadly allowed for Liability-Avoidance and Investigatory Purposes and limited to the PJR for Business Purposes, all borderline monitoring practices must only be allowed where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Monitoring Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). The following three of the top monitoring practices are classified as borderline:

1. E-mail & Text Message Monitoring;
2. GPS & RFID Monitoring; and
3. Physical Searches

### E-MAIL & TEXT MESSAGE MONITORING

E-mail monitoring is one of the most analyzed topics in the workplace privacy literature.<sup>202</sup> Despite its many critiques, companies are wise to join the forty-three percent of businesses who currently monitor employee e-mail.<sup>203</sup> A recent iteration of e-mail - text messaging - is new enough that few studies or cases even mention the practice.<sup>204</sup> Because texting is similar in nature to e-mail and because monitoring text messages has become a hot topic (the case of *City of Ontario v. Quon* was recently argued in the Supreme Court),<sup>205</sup> this monitoring practice is also considered in this section.

E-mail monitoring is a powerful liability-prevention tool because e-mail: (1) creates a permanent record useful against a company in a lawsuit, (2) is quickly and efficiently transmitted inside and outside a company and (3) is impersonal by nature and rife for abuse. For example, employees do not realize the power of e-mail as “Exhibit A” in a lawsuit targeting either them or their employer. An attorney in possession of e-mail correspondence is akin to a prosecutor holding DNA evidence - it can be the

---

<sup>202</sup> A Lexis Nexis search for the phrase “e-mail monitoring” produced 256 articles as of May 23, 2010.

<sup>203</sup> See e.g., *2007 AMA Survey*, *supra* note 2, at 4 (showing that 26% of employers monitor all employees and 17% monitor only selected job categories).

<sup>204</sup> See generally, *See 2007 AMA Survey*, *supra* note 2 (covering many of the relevant monitoring practices but omitting text message monitoring).

<sup>205</sup> *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 910 (9th Cir. 2008) (holding that the “search of [the employees’] text messages violated their Fourth Amendment and California constitutional privacy rights because they had a reasonable expectation of privacy in the content of the text messages, and the search was unreasonable in scope.”). The Supreme Court heard oral arguments in this case in April 2010. See e.g., Erin Miller, *Podcast: City of Ontario v. Quon*, SCOTUSBLOG.COM, April 19, 2010, available at <http://www.scotusblog.com/2010/04/podcast-city-of-ontario-v-quon/>. Although the technologies differ, they are close enough for the term e-mail to encompass text messages for the purposes of this section.

smoking gun that dooms a defendant at trial.<sup>206</sup> In fact, twenty-four percent of employers have been forced to turn over employee e-mail to courts or regulators and fifteen percent “have battled workplace lawsuits triggered by employee e-mail.”<sup>207</sup> These statistics prove that employers must glean some idea about who their employees e-mail and how their employees communicate over e-mail. Additionally, companies that implement an e-mail monitoring policy must make certain it is thorough. Employers with e-mail policies will be held to account if they fail to discover suspicious/malicious statements communicated over their network.<sup>208</sup>

The negative implications on morale are too high, however, for employers to monitor every e-mail sent and received over company servers.<sup>209</sup> Problematically, forty percent of companies claim to have individuals from Human Resources, Legal and Compliance Departments read employee e-mail.<sup>210</sup> This human monitoring is much more invasive than e-mail monitoring software which can scan e-mail for suspicious/malicious language and flag it for Information Technology professionals. Having liability-prevention departments such as Legal monitor e-mail is morale-defeating and smells like Big Brother actively seeking violations of company policy.<sup>211</sup> This form of monitoring will offend the vast majority of employees who work consistently in the best interests of their employer. In turn, these loyal employees will be reluctant to use company e-mail systems for even the most benign work-related purposes. Slowly, this decrease in trust and morale will lead to a decrease in productivity and corporate efficiency.

---

<sup>206</sup> See *id.*

<sup>207</sup> 2007 AMA Survey, *supra* note 2, at 2 (citing another AMA study and stating that concern “over litigation and the role electronic evidence plays in lawsuits and regulatory investigations has spurred more employers to monitor online activity. Data security and employee productivity concerns also motivate employers to monitor Web and e-mail use and content. Workers’ e-mail and other electronically stored information create written business records that are the electronic equivalent of DNA evidence.”).

<sup>208</sup> See *e.g.*, Peter J. Bezek, Shawn M. Britton and Robert A. Curtis, *Employer Monitoring Of Employee Internet Use And E-Mail: Nightmare Or Necessity?*, 2:11 MEALY’S CYBER TECH LITIGATION REPORT, (January 2001), available at [www.foleybezek.com/art.InternetFile.pdf](http://www.foleybezek.com/art.InternetFile.pdf) (last visited May 3, 2010) [hereinafter *Nightmare or Necessity*] (reiterating the idea that:

[I]f an employer undertakes monitoring, he may have a higher duty to ensure that no offensive, harassing, or otherwise inappropriate material remains on the system. As [courts have noted], “employers do not have a duty to monitor private communications of their employees; employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment.” When an employer monitors, it is more likely that it will be deemed to have knowledge of harassing material. If no action is taken, this could result in direct liability for the employer. Thus, once an employer commences monitoring, it must do so continuously and purposefully or risk increased liability.”)

(internal citations omitted).

<sup>209</sup> See *id.* at 4 (stating that “if an employer’s policy is to monitor e-mail, there is no basis for employees to have an expectation of privacy. In addition to helping create a higher duty for ensuring that the system is not used for inappropriate purposes, the lack of an expectation of privacy can create problems with employee morale. Studies have shown that employees who are monitored in various ways have increased stress and fatigue, higher absenteeism, and lower morale. Perhaps it is common sense; no one feels good knowing that he is being ‘watched.’”).

<sup>210</sup> See 2007 AMA Survey, *supra* note 2, at 5.

<sup>211</sup> See *e.g.*, Thomas York, *Invasion Of Privacy? E-Mail Monitoring Is On The Rise*, INFORMATION WEEK, Feb. 21, 2000 available at <http://www.informationweek.com/774/email.htm> (last visited May 3, 2010) (stating that e-mail monitoring issues “have also saddled IT managers with duties that go beyond routine support and maintenance of E-mail systems to include enforcement of policies that help protect companies against claims of sexual and racial harassment.”).

With these pros and cons in mind, a new monitoring regime should allow companies to reap the benefits of e-mail monitoring for all three Monitoring Purposes. This tracks current precedent which allows employers to monitor e-mail broadly - even when management promises they will do no such thing.<sup>212</sup> However, a new regime should pare back this precedent a bit considering the increasing invasiveness of contemporary e-mail monitoring technology. As with other borderline monitoring technologies, the privacy judgment rule should limit employer e-mail monitoring to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Monitoring Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s).<sup>213</sup>

An employer's reasonable judgment in these cases should allow management to monitor e-mail to look for keywords likely to trigger litigation,<sup>214</sup> discover large file transmissions that impair the employer's system and discover workplace policy violations by employees under investigation or on probation. Although a new legal regime should not force employers to micromanage the monitoring process, wise managers will not monitor e-mail merely to gauge employee efficiency or morale. Additionally, absent an investigation, e-mail should not be read by individuals in non-technology-related departments looking for random violations. There are less invasive, more narrowly tailored ways to discover employee misconduct such as periodic evaluations of employee work product, in person inquiries or prominent complaint procedures. Based on the problems identified in this section, e-mail monitoring must be considered a borderline practice and regulated as such.

## GPS & RFID MONITORING

---

<sup>212</sup> See e.g., *Smyth v. Pillsbury*, 914 F. Supp. 97, 98 & 101 (E.D. Pa. 1996) (holding that an employee did not enjoy a reasonable expectation of privacy in e-mail sent over an employer's system - even though the employer's policy stated that management would not monitor employee e-mail and that it would remain confidential.).

<sup>213</sup> Courts are likely to approve of this standard as it approximates several workplace privacy standards. National Workrights Institute, *On Your Tracks: GPS Tracking in the Workplace*, 22, available at [www.workrights.org/issue\\_electronic/NWI\\_GPS\\_Report.pdf](http://www.workrights.org/issue_electronic/NWI_GPS_Report.pdf) (last visited May 23, 2010) [hereinafter *On Your Tracks*] (stating that:

In determining whether workplace related monitoring violates a protected right, courts will often first evaluate whether the monitoring is job-related. Some courts use a nexus test to determine whether the employer's action is sufficiently related to a job function of the employee or their fitness to perform a job function. If so courts will attempt to balance the employer's need for information with the employees [sic] privacy rights. The nature of the employees [sic] job and the degree of importance of the information obtained by the employer are lengthy and fact sensitive determinations that weigh heavily towards determining whether the employer acted properly. Where the job implicates issues of safety, for example, and the nature of the information sought is directly related to ensuring that the individual is properly suited to ensure such, the employer will be in a good position to defend a claim. The employer must still show that their actions were not overbroad.).

(internal citations omitted).

<sup>214</sup> These are words that indicate ongoing sexual, gender or racial-based harassment, impending violence related to the workplace or employees, or anything else that would trigger liability under the law. Software exists to conduct just this type of monitoring. See e.g., *Nightmare or Necessity*, *supra* note 208, at 5 (discussing e-mail monitoring software that can search for keywords and stating that this "type of software searches outgoing and incoming e-mails for certain keywords or file types. For example, this software can be programmed to scan outgoing e-mails for curse words or attached pictures and then prevent the e-mail from being sent and simultaneously forward those emails to the system administrator for review. Software of this type can range from \$200 to \$1,000.").

Contemporary GPS and RFID technology allows employers to do much more than obtain directions and locate inventory. This powerful monitoring practice can also serve as a dead-on employee locator beacon. As detailed in Part III, these trackers can be placed covertly on company equipment such as cars, forklifts and cellular phones or on company employees in the form of Smart ID cards/badges. For obvious reasons, tracking employer property is less invasive than tracking employee movements or locations. The problem is that tracking employer property often also tracks employees carrying or moving along with such property. The most problematic use of GPS/RFID technology involves tracking the movements or locations of employees who are not operating or moving along with company property. Regardless of the Monitoring Purpose for which it is utilized, employees dislike this type of monitoring whether used on their equipment or their persons. A recent article cataloged the silent invasiveness of GPS/RFID monitoring rather succinctly:

Many times people take for granted the inherent right to go throughout the world undetected. When an employee's location is tracked in real time, he no longer has any real sense of privacy. His employer reviews every decision he makes, whether it is to take the dog for a walk or to go to a local town meeting. Each tracked location acts like a piece of a puzzle to the worker's life. After tracking an employee's location for a length of time, the employer will know that the worker leaves his home every day at 8:00am. He will know that on his way to work he stops at the local convenience store for a donut and goes to work. In addition, he will find that he takes two bathroom breaks during the day, one at 10:00 and one at 3:00. After work, it will be no secret that this employee stops to pray at his synagogue on his way home and then spends three hours at the house of his girlfriend, who happens to be an ex-employee. At the end of the day, the employer will have enough pieces of the puzzle to create a fully fleshed out picture of the off-duty life of his employee. Extremely personal and private details of an employee's life are revealed, including their political activities, physical and mental health and relationships.<sup>215</sup>

Employers appear to understand the invasiveness of GPS/RFID technology and avoid it or, perhaps, employers have merely been slow to adopt the technology. Regardless, only eight percent of companies track employee property, three percent monitor employee cell phones and one percent track employee ID badges.<sup>216</sup> Recall that the required notification provisions that must be part of any new regime will intensify the invasiveness when employees become aware their employer is utilizing GPS/RFID technology.<sup>217</sup>

There is little doubt that the enterprise protection provided by GPS/RFID technology is high. It is always important for employers to understand where their property is located - especially in cases of theft. In addition, in many industries it is crucial to know where employees are located along their routes or itineraries. These benefits are countered by the outrage and invasiveness caused when

---

<sup>215</sup> *On Your Tracks*, *supra* note 213, at 19.

<sup>216</sup> See *2007 AMA Survey*, *supra* note 2, at 3 (stating that employers "have been slow to adopt emerging monitoring/surveillance technologies to help track employee productivity and movement. Employers who use Assisted Global Positioning or Global Positioning Systems satellite technology are in the minority, with only 8% using GPS to track company vehicles; 3% using GPS to monitor cell phones; and less than 1% using GPS to monitor employee ID/Smartcards.").

<sup>217</sup> The notice requirement will force companies to disclose such monitoring and face the employee resentment that is sure to follow. See e.g., Ben Charny, *Big Boss is Watching*, CNET NEWS.COM, Sept. 24, 2004, [http://news.cnet.com/Big-boss-is-watching/2100-1036\\_3-5379953.html](http://news.cnet.com/Big-boss-is-watching/2100-1036_3-5379953.html) (stating that one of "the earliest examples of how an employer can walk this fine line is in Chicago, where about 500 city employees now carry geo-tracking phones, mainly as a tool to increase their productivity. The phones were distributed to employees only after their unions won several concessions, including allowing workers to shut down geo-tracking features during lunch time and after hours.").

employees discover that their every move and location is tracked. Because there is little case law to set a precedent in this area, a new regime can protect employees from scratch - a luxury not offered in many of the other monitoring areas.<sup>218</sup> As with the other borderline monitoring practices, a new regime should allow GPS/RFID monitoring of employees for all three Monitoring Purposes. However, such monitoring should be limited to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Monitoring Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). This new standard would require employers to turn off GPS/RFID locators while employees are on break or at lunch - where few if any Monitoring Purposes are implicated. Wise employers, pondering the privacy judgment rule, will also do more than just disclose the implementation of this technology with their employees - they will work with them to tailor a solution that meets the interests of both parties.

## PHYSICAL SEARCHES

Employers who physically search through employee offices or property ask for trouble. This is true even if the employer pays the rent and provides the equipment. Such searches happen often, however, as management seeks information pertaining to all three Monitoring Purposes.<sup>219</sup> Trouble lurks because employees quickly develop expectations of privacy in these areas - expectations that courts find reasonable even when employees know they are monitored.<sup>220</sup> Long before sophisticated monitoring technology was able to covertly invade every nook and cranny of an employee's space, the Supreme Court made the case for why such expectations were reasonable:

Finally and most importantly, the reality of work in modern time, whether done by public or private employees, reveals why [an] employee's expectation of privacy in the workplace should be carefully safeguarded and not lightly set aside. It is, unfortunately, all too true that the workplace has become another home for most working Americans. Many employees spend the better part of their days and much of their evenings at work.<sup>221</sup>

Today, employers who search employee spaces or property are wise to consider the following factors: (1) the intrusiveness of the search, (2) the type of property/place to be searched, (3) whether notice was given, (4) whether consent was obtained, (5) who will conduct the search (6) how will the search be conducted (including the monitoring technology involved), (7) what business justification allows for the search and (8) whether the employee has a reasonable expectation of privacy in the property/place.<sup>222</sup> This analysis requires a great deal of intuition and information as employers struggle to accurately

---

<sup>218</sup> See e.g., *On Your Tracks*, *supra* note 213, at 21 (stating that “[w]hile there is no case law on GPS monitoring in the workplace, there are guidelines to pursuing litigation in this area that can be derived from existing case law on workplace privacy, privacy generally and the use of technology to monitor individuals.”).

<sup>219</sup> See e.g., Richard A. Bales and Jeffrey A. McCormick, *Workplace Investigations in Ohio*, 30 CAP. U. L. REV. 29, 89 (2002) [hereinafter *Workplace Investigations*] (stating that employers “have a variety of different reasons for conducting workplace searches, such as investigating employee theft, maintaining workplace security, and locating misplaced files and documents.”) (internal citations omitted).

<sup>220</sup> See *id.* (stating that employees “have a reasonable right not to be subjected to unreasonably intrusive searches, and an employer who transgresses this line may be exposed to liability for the tort of intrusion.”) (internal citations omitted).

<sup>221</sup> *Ortega*, *supra* note 51, at 739 (Blackmun, J. dissenting).

<sup>222</sup> See *id.*

assess each element. Making matters more difficult is a Supreme Court opinion that lawsuits stemming from physical searches should be adjudicated on a case-by-case basis.<sup>223</sup> These legal and logistical headaches, combined with the extreme invasiveness involved in violating another person's space, demonstrate why physical searches are classified as borderline monitoring practices.

Courts generally uphold searches of office space and other company-provided property located on an employer's premises.<sup>224</sup> This is especially true as the object of the search moves further away from being an extremely private place (i.e., employee locker) or a private possession (i.e., briefcase). Under this sliding scale approach, it would be more permissible to search an employee's cubicle than office, better to search through an employee's desk drawers than mail.<sup>225</sup> On the contrary, courts have recognized that the personal belongings employees bring to the workplace are more private than employer property and should not be searched absent compelling circumstances.<sup>226</sup>

A new monitoring regime must add some clarity by allowing physical searches for all three Monitoring Purposes but limiting the practice to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Monitoring Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). This standard is similar to a statement in the *Ortega* opinion that “[o]rdinarily, a search of an employee's office by a supervisor will be ‘justified at its inception’ when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file.”<sup>227</sup>

---

<sup>223</sup> *Ortega*, *supra* note 51, at 718 (stating that “[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.”). Although *Ortega* dealt with a public sector employee protected by the Fourth Amendment, state and federal appellate courts are likely to use *Ortega* as a starting point for cases involving searches by private employers.

<sup>224</sup> See e.g., *Doe v. XYC Corp.*, 887 A.2d 1156, (N.J. Ct. App. 2005). In *Doe*, the court looked into three areas to determine if the monitoring was legal. First, the court looked to whether the employer had the capability to monitor. See *id.* at 1164 (holding that the suspect's “immediate supervisor, [searched through the employee's] computer while he was at lunch and clicked on ‘websites visited.’ . . . [N]one of the sites identified were actually explored and no further action was taken to determine the nature of Employee's pornographic related computer activities. Instead, [the supervisor] was simply instructed to tell Employee to stop whatever he was doing. Thus, defendant's capability to monitor Employee's activities on his work computer was clearly established.”). The court then looked to whether the employee had a legitimate expectation of privacy. See *id.* at 1166 (holding that the employee's “office, as with others in the same area, did not have a door and his computer screen was visible from the hallway, unless he took affirmative action to block it. Under those circumstances, we readily conclude that Employee had no legitimate expectation of privacy that would prevent his employer from accessing his computer to determine if he was using it to view adult or child pornography.”). Finally, the court analyzed whether the employer had a right to search the office to investigate an employee's computer use. See *id.* at 1166 (concluding that the employer, “through its supervisory/management personnel, was on notice that Employee was viewing pornography on his computer and, indeed, that this included child pornography [and thus had a duty to investigate].”).

<sup>225</sup> See *id.* at 1159-1169.

<sup>226</sup> See e.g., *Borse v. Piece Goods Shop, Inc.* 963 F.2d 611, 628 (3rd Cir. 1992) (holding that “dismissing an employee who refused to consent to . . . personal property searches would violate public policy if the [searching] tortiously invaded the employee's privacy.”). *Borse* dealt with a “consent to search personal property” form and not an actual search - promoting the idea that courts generally frown upon searches of an employee's personal property. *Id.* at 613 (stating that “Borse was employed as a sales clerk by the Piece Goods Shop for almost fifteen years. In January 1990, the Shop adopted a drug and alcohol policy which required its employees to sign a form giving their consent to urinalysis screening for drug use and to searches of their personal property located on the Shop's premises. Borse refused to sign the consent form.”).

<sup>227</sup> *Ortega*, *supra* note 51, at 726.

In *Ortega*, Justice Scalia claimed that such physical searches to retain files or prevent liability are “regarded as reasonable and normal [in private workplaces].”<sup>228</sup> The extra protection added under the new regime can be justified by the increasingly-sophisticated manner in which employers are able to conduct physical searches. In 1987 - the time frame surrounding *Ortega* - the search process was simple: management would walk into the office and manually look through desk drawers and files. In 2010, employers can still enter employee spaces to manually search desk drawer and files AND can additionally analyze the complete contents of an employee’s personal laptop, Internet browser, or cellular phone within minutes.

As a caveat, a new regime should prohibit employers from conducting body searches of employees,<sup>229</sup> searching employee homes (even after obtaining consent)<sup>230</sup> or holding employees against their will.<sup>231</sup> The privacy judgment rule should call for employers to turn such matters over to the authorities. Finally, a regime should allow employers to seize employee property only when: (1) the item poses an immediate danger to the employee or others in the workplace, (2) possession of the item in the workplace conflicts with an employer’s policy and (3) such policy is supported by a reasonable business judgment.<sup>232</sup> Employers unsatisfied with an employee’s choice to bring a non-dangerous item to work can send the employee home and/or utilize termination remedies under the employment at will doctrine - all without seizing any property.

## **E. CATEGORY FOUR: POOR PRACTICES**

This article argues throughout that increasingly-sophisticated monitoring technology will soon require courts to redraw the “reasonable expectation of privacy” line. As new, high-tech invasions of privacy generate outrage and serious lawsuits, courts are likely to seek balance by enhancing employee privacy rights. One of the first areas to shift will likely be the monitoring technologies that fall into category four - poor practices. With this prediction as a guide, a new monitoring regime should: (1) prohibit these monitoring techniques from being utilized for Business and Liability-Avoidance Purposes and (2) only allow these monitoring techniques during an investigation to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Investigatory Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). The rationale behind this prohibition is that the invasions that stem from poor monitoring practices are

---

<sup>228</sup> *Id.* at 732 (Scalia, J. concurring).

<sup>229</sup> See e.g., *Ogborn v. McDonald's Corp.*, No. 04-CI-00769 (Ky. Cir. Ct. Bullitt County Oct. 5, 2007) (awarding \$6.1 million to an 18-year old McDonald’s employee who was strip-searched by an assistant manager at the request of a third party posing as a police officer investigating a theft) and *McDonald's Corp v. Ogborn*, 2009 WL 3877533 (Ky. App. Nov. 20, 2009) [hereinafter *Ogborn*] (upholding most of the damages imposed against McDonald’s in the trial court).

<sup>230</sup> See e.g., *Wal-Mart Stores, Inc. v. Lee*, 74 S.W.3d 634, 648-49 (Ark. 2002) (upholding a jury verdict finding that an employer who gained consent to search an employee’s home during a theft investigation committed the tort of intrusion upon seclusion).

<sup>231</sup> See *Ogborn*, *supra* note 229, at 19 (stating that the “record shows there was sufficient and substantial evidence to submit the case to the jury on this cause of action. Ogborn’s evidence shows that she was, in fact, forcibly and unlawfully detained [and that the jury’s finding of false imprisonment was reasonable].”).

<sup>232</sup> For example, an employer should be able to seize a handgun brought to work by an employee in violation of the employer’s anti-violence policy. If an employee shows up with alcohol or drugs, however, employers are wise to send the employee home or impose other disciplinary action rather than trying to seize the property.

excessive and there are more effective, less-invasive ways for employers to protect their interests. The four monitoring practices classified as poor include:

1. Desktop Monitoring;
2. Keystroke Monitoring;
3. Phone & Voicemail Monitoring; and
4. Video Surveillance

## **DESKTOP MONITORING & KEYSTROKE MONITORING**

Desktop and keystroke monitoring are closely related and will be examined together. This technology cheaply and rapidly catalogues employee work product and work flow over time. For example, employers can decipher the precise contents of correspondence created, sent or received on a work computer. Desktop and keystroke technology can also flag sexually-charged or violently keywords or content traveling over the company network and/or keep track of the number of times an employee hits delete or edits a document. The flip side is that monitoring an employee's electronic footprint in this manner is extremely invasive and can paint an incomplete picture. For example, many very productive employees are poor typists, hit delete/backspace numerous times when drafting or edit work product multiple times before submission.<sup>233</sup> Many very productive employees also employ unique workflows that desktop and keystroke monitoring cannot evaluate accurately. Finally, when employees become aware that their employer is monitoring their computer, either before or after the fact, the negative repercussions on morale and dignity greatly outweigh the benefits mentioned above.<sup>234</sup>

During an investigation, however, the need for information created on a work computer becomes more compelling. Employers may need to access e-mails from a rogue employee's personal account to prove a theft of trade secrets or online sexual harassment. Employers may also need to use an employee's drafting speed, typing accuracy, or misuse of company time to show a lack of productivity in an wrongful termination lawsuit. Therefore, as mentioned above, a new monitoring regime should allow desktop and keystroke monitoring, only during the course of an investigation or lawsuit.

---

<sup>233</sup> I am a very productive employee (i.e., in year six of six in the tenure process) who is definitely guilty of poor typing skills. With this in mind, I would be terrified if my employer was able to watch me type or edit a document. The practice is in no one's best interest whether it be in my case or in the case of any productive employee.

<sup>234</sup> Specific web pages exist to help people determine whether a third party, such as an employer, is monitoring their desktop or keystrokes. See e.g., *How to Detect Computer and E-Mail Monitoring or Spying Software*, ONLINE TECH TIPS, <http://www.online-tech-tips.com/computer-tips/how-to-detect-computer-email-monitoring-or-spying-software/> (last visited May 18, 2010). The text from an advertisement for a desktop monitoring program helps demonstrate how such programs might negatively impact morale:

Owners who are serious about proper employee management use these tools to keep a close watch on each and every activity of the employees online. Every business faces issues related to employee management time to time, that can be resolved only with a pc monitoring software. . . . With Employee Desktop LIVE Viewing software you can monitor 'n' number of computers at once and the target users will never know as this PC monitoring tool remains invisible and completely under your control.

*Employee Management with PC Monitoring Tool*, TRCB.COM, <http://www.trcb.com/computers-and-technology/data-recovery/employee-management-with-pc-monitoring-tool-24004.htm> (last visited May 18, 2010).

Some members of Congress are aware of the invasiveness of desktop and keystroke monitoring - at least in the related arena of information privacy. In 2007, the House of Representatives passed legislation that prohibited unfair and deceptive practices by third parties utilizing keyloggers to collect personal information.<sup>235</sup> The Securely Protect Yourself Against Cyber Trespass Act (or the SPY Act) passed the House then died in the Senate at the end of the 110th Congress.<sup>236</sup> The court system has also been hampered because few litigated cases revolve around either of these monitoring techniques.

A criminal case, styled *United States v. Scarfo*, touched on keystroke monitoring implemented by the federal government in the interests of national security.<sup>237</sup> In *Scarfo*, the FBI covertly installed a keylogging device on the suspect's (Scarfo's) computer looking for evidence of illegal gambling and loansharking.<sup>238</sup> The keylogger recorded his passwords for FBI agents who then logged-in to the computer and found incriminating evidence.<sup>239</sup> Scarfo brought a motion to suppress the evidence under the wiretapping prohibitions of the ECPA, which was denied due to the ECPA's weak privacy protections.<sup>240</sup> The court, in dicta, stated that the "case presents an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity."<sup>241</sup> It will be interesting to see how courts use the *Scarfo* precedent in employment law cases which do not typically involve national security. Another recent case, also outside of the employment arena, occurred when a public school district installed a program called Theft Tracker on 2,000 student computers.<sup>242</sup> When activated, "the program records the laptop's Internet address, captures an image of anything on the computer's screen, and takes a Webcam photo every fifteen minutes until the program is deactivated."<sup>243</sup> Students, parents and the community were outraged when the monitoring was

---

<sup>235</sup> See H.R. 964, 110th Cong. (2007) (formerly H.R. 29 (2005) and H.R. 2929 (2006)), available at <http://www.govtrack.us/congress/billtext.xpd?bill=h110-964> (last visited May 18, 2010). The law would prohibit a person who is not the owner or authorized user of a computer to engage in unfair or deceptive practices that involve collecting "personally identifiable information through the use of a keystroke logging function." *Id.* at § 2(a)(3).

<sup>236</sup> See *HR 964: Securely Protect Yourself Against Cyber Trespass Act*, GOVTRACK.COM, <http://www.govtrack.us/congress/bill.xpd?bill=h110-964> (last visited May 18, 2010) (stating that this "bill passed in the House of Representatives by roll call vote. The vote was held under a suspension of the rules to cut debate short and pass the bill, needing a two-thirds majority. This usually occurs for non-controversial legislation. The totals were 368 Ayes, 48 Nays, 16 Present/Not Voting."). A Senate vote never occurred and the bill died at the end of the session. *Id.*

<sup>237</sup> 180 F. Supp. 2d 572 (D. N.J. 2001) [hereinafter *Scarfo*]. The court stated that "[i]t appears that no district court in the country has addressed a similar issue. Of course, the matter takes on added importance in light of recent events and potential national security implications." *Id.* at 574.

<sup>238</sup> See *id.* at 574.

<sup>239</sup> *Id.*

<sup>240</sup> *Id.* at 581-583 (stating that the keylogger, "which is the exclusive property of the F.B.I., was devised by F.B.I. engineers using previously developed techniques in order to obtain a target's key and key-related information. As part of the investigation into Scarfo's computer, the F.B.I. 'did not install and operate any component which would search for and record data entering or exiting the computer from the transmission pathway through the modem attached to the computer.'" (internal citations omitted).

<sup>241</sup> *Id.* at 574.

<sup>242</sup> See e.g., Workplace Privacy Counsel, *School District's Woes from Using Webcams to Track School-Issued Laptops Should Be an Eye-Opener for Employers*, PRIVACYBLOG.LITTER.COM, April 27, 2010, <http://privacyblog.littler.com/2010/04/articles/electronic-monitoring/school-districts-woes-from-using-webcams-to-track-schoolissued-laptops-should-be-an-eyeopener-for-employers/#more>.

<sup>243</sup> *Id.*

discovered and at least one class action lawsuit has been filed to date.<sup>244</sup> Although the outrage was targeted primarily towards the 56,000 pictures that were taken via the video surveillance component, the desktop monitoring component was also very unpopular.<sup>245</sup>

With this extreme invasiveness in mind, a new monitoring regime should prohibit the use of desktop and keystroke monitoring outside of the investigatory context. As with the rest of the poor monitoring practices listed in this section, there are less intrusive ways for employers to obtain the same liability protection. For example, non-productive employees stand out and management need not monitor keystrokes or desktops for proof of sloth or incompetence. In addition, although the ability to identify and stop sexual harassment or workplace bullying is important, there are more powerful weapons available to accomplish these goals such as strong, well-communicated anti-harassment or non-violence policies. During an investigation, employers should be allowed to use this technology, without notifying employees, as long as it is limited to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Investigatory Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s).

## PHONE & VOICEMAIL MONITORING

Aural monitoring technology has advanced to the point where employers can place tiny listening devices into employee computers, phones, vehicles and even identification badges. Contemporary technology is at odds with current law because employees have a reasonable expectation of privacy in most of the personal conversations they have at work. In fact, the law generally allows employers to listen to a conversation until they recognize that it is personal - then they must cease and desist.<sup>246</sup> Courts have gone even further by holding that an employee might have a reasonable expectation of privacy in phone calls that can be overheard by co-workers without the aid of technology. The idea is that even the most reasonable employees do not expect their personal conversations to be monitored at work. Although aural technology grants employers the ability to blanket the workplace and hear everything, such monitoring is unable to determine when a conversation is personal and disconnect.

---

<sup>244</sup> *Id.* The lawsuit is styled *Robbins v. Lower Merion School District* and was filed in the Eastern District of Pennsylvania. *Id.* The case has been described as follows:

Plaintiffs, Michael E. and Holly S. Robbins, bring this action on their own behalf and on behalf of their minor son, Blake J. Robbins, and as a Class Action on behalf of a class consisting of Plaintiffs and all other students, together with their parents and families (the "Class"), who have been issued a personal laptop computer equipped with a web camera ("webcam") by the Lower Merion School District. Plaintiffs and the Class seek to recover damages caused to the Plaintiffs and Class by Defendants' invasion of Plaintiffs' privacy, theft of Plaintiffs' private information and unlawful interception and access to acquired and exported data and other stored electronic communications in violation of the Electronic Communications Privacy Act, The Computer Fraud Abuse Act, the Stored Communications Act, § 1983 of the Civil Rights Act, The Fourth Amendment of the United States Constitution, the Pennsylvania Wiretapping and Electronic Surveillance Act and Pennsylvania common law.

Mark S. Haltzman, et. al., *Blake J. Robbins v. Lower Merion School District*, HEARTLAND.ORG, Feb. 11, 2010, [http://www.heartland.org/policybot/results/27289/Blake\\_J\\_Robbins\\_v\\_Lower\\_Merion\\_School\\_District.html](http://www.heartland.org/policybot/results/27289/Blake_J_Robbins_v_Lower_Merion_School_District.html).

<sup>245</sup> *Id.*

<sup>246</sup> See e.g., *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 583 (11<sup>th</sup> Cir. 1983).

Recall that the ECPA requires only one party to a conversation to agree for the aural monitoring to be legal. Many state privacy acts go further than the ECPA, however, and hold that all parties to a private conversation must agree to monitoring.<sup>247</sup> This dual-consent provision is an important requirement that should be retained in a new regime because it notifies employees that monitoring will take place and allows them the freedom to act accordingly. States with dual consent provisions are increasing in number and it appears that legislatures and courts are moving the sliding scale of protection towards employees when it comes to aural monitoring. Each of these reasons demonstrates why phone and voicemail monitoring is classified as a poor monitoring practice.

Considering the sophistication and invasiveness of aural monitoring, a new monitoring regime should ban the use of aural monitoring other than during the course of an investigation unless all parties to the monitoring consent. The situation is different during an investigation and, therefore, employers should not be required to obtain informed consent for investigatory matters.<sup>248</sup> The monitoring should be limited to cases where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Investigatory Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). This compromise attempts to balance the employer's right to protect itself from liability (particularly when it can make a case for an investigation) with the employee's right to privacy in personal conversations conducted at the workplace. Nothing in the new regime would stop the employment-at-will doctrine from allowing employers to terminate employees who conduct personal conversations in the workplace - even if management cannot listen to the entire conversation.

## VIDEO SURVEILLANCE

Today's video surveillance is not your mother's video surveillance. Miniscule cameras can be hidden discretely inside laptops, mirrors, offices and other company property - often unbenounced to

---

<sup>247</sup> See e.g., CAL. PEN. CODE § 631(a) (Deering 2008) (providing for "criminal penalties for any person who 'intentionally taps, or makes any unauthorized connection . . . with any . . . telephone wire, line, cable, or instrument,' including those of 'any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit' or who 'uses, or attempts to use, . . . or to communicate' information so obtained, or who 'aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause' such acts to be done."). Conversations that are not reasonably private are a different story and even California law allows some monitoring. See e.g., *Wilkins v. NBC, Inc.*, 71 Cal. App. 4th 1066 (Cal. Ct. App. 1999). The penalties for violating the California Privacy Act are severe:

A first offense . . . is punishable by a fine of up to \$2,500 and imprisonment for no more than one year. Subsequent offenses carry a maximum fine of \$10,000 and jail sentence of up to one year. Intercepting, recording, and disclosing information each carries a separate penalty. . . . Anyone injured by a violation of the laws against disclosure of telegraphic or telephonic messages can recover civil damages of \$5,000 or three times actual damages, whichever is greater. A civil action for invasion of privacy also may be brought against the person who committed the violation.

CAL. PEN. CODE § 637.2(a) (Deering 2008).

<sup>248</sup> If the employer determines that the communication is personal and outside of the scope of the investigation, it must cease and desist from monitoring. Knowing that a personal communication occurred is more than enough to take adverse employment action in such situations under the employment-at-will doctrine.

employees.<sup>249</sup> Although such technology allows low-cost, around-the-clock enterprise protection, the invasion of privacy involved is tremendous. Sophisticated cameras record employee movements, statements and missteps with great clarity. This technology can also be used to monitor employees in places where they have little expectation of being monitored - such as working from home or from the hotel pool.<sup>250</sup>

Because video surveillance of employees can quickly become excessively invasive - even during the course of a pending investigation - it is classified as a poor employment practice. On the other hand, video surveillance of employer property - such as parking lots and exits is not nearly as problematic and even wise. This technology crosses the reasonable expectation of privacy line in most situations when targeted directly at employees instead of property. For example, a recent court considering video surveillance stated: "We pause here to add that there is no question the defendants' twenty-four hour video surveillance of the entire office was unnecessarily broad for the limited investigation of alleged criminal activity occurring in the office after hours."<sup>251</sup> That same court was hesitant, however, to ban such monitoring stating that "the office . . . was open to the public. The office was not limited to the plaintiff's exclusive use, and the over-all public exposure of the physical layout abrogated any expectation that her actions, while in the office, would be private."<sup>252</sup> In the same vein, another court upheld video monitoring of an office after business hours.<sup>253</sup> The employer worried that another employee was sneaking into the office to view pornography on a company computer and recorded activity within the office only after hours.<sup>254</sup> Although the court upheld the monitoring because the plaintiff employees who occupied the office during work hours were never caught on the tape, the opinion stated that:

---

<sup>249</sup> See e.g., Michael Baroni, *Employee Privacy in the High-Tech World*, 48 ORANGE CTY. LAWYER 18, 18 (May 2006) (stating that "laptops and computer monitors now come with tiny cameras embedded in the frame of the computer screen. Company cars can also be easily equipped with spy-cams, as well as almost every object in an office from a plant to a lamp.").

<sup>250</sup> *Id.* (stating that most employees "would be less than enthusiastic about possibly being watched every second - particularly those who work outside of the traditional office. Imagine an un-showered home-office employee working on a computer in his or her underwear, or an employee using a company van for extra-marital trysts, or a traveling salesman catching up on e-mails from a hotel bar, all being watched without their knowledge. . . not a pretty sight.").

<sup>251</sup> *Nelson v. Salem State College*, 845 N.E.2d 328, 347 (Mass. 2006).

<sup>252</sup> *Id.* (holding that "[a]lthough . . . the plaintiff lacked notice of the defendants' surveillance of the office, the facts of this case, including the explicitly public nature of the work conducted . . . and the ready visual and physical access that was afforded the public, all employees (including management) and volunteers . . . abrogated any objectively reasonable expectation of privacy."). See generally *California v. Gibbons*, 215 Cal. App. 3d 1204 (Cal. Ct. App. 1989).

<sup>253</sup> See *Hernandez v. Hillsides*, 211 P.3d 1063, 1082 (Cal. 2009) [hereinafter *Hillsides*].

<sup>254</sup> *Id.* at 1066 (stating that:

[Hitchcock], the director of the facility, learned that late at night, after plaintiffs had left the premises, an unknown person had repeatedly used a computer in plaintiffs' office to access the Internet and view pornographic Web sites. Such use conflicted with company policy and with Hillsides's aim of providing a safe haven for the children. Concerned that the culprit might be a staff member who worked with the children, and without notifying plaintiffs, Hitchcock set up a hidden camera in their office. The camera could be made operable from a remote location, at any time of day or night, to permit either live viewing or videotaping of activities around the targeted workstation. It is undisputed that the camera was not operated for either of these purposes during business hours, and, as a consequence, that plaintiffs' activities in the office were not viewed or recorded by means of the surveillance system. Hitchcock did not expect or intend to catch plaintiffs on tape.).

We appreciate plaintiffs' dismay over the discovery of video equipment—small, blinking, and hot to the touch—that their employer had hidden among their personal effects in an office that was reasonably secluded from public access and view. Nothing we say here is meant to encourage such surveillance measures, particularly in the absence of adequate notice to persons within camera range that their actions may be viewed and taped.<sup>255</sup>

The court required that the use of the video technology be “narrowly tailored in place, time and scope and [be] prompted by legitimate business concerns.”<sup>256</sup> For the reasons expressed above, many states ban the use of video cameras in especially private places such as bathrooms and locker rooms. Precedent generally allows for video surveillance in non-private places as long as employers can produce a legitimate business reason.

With this in mind, a new monitoring regime must balance the fact that employees have a reduced expectation of privacy in the workplace and the fact that video surveillance is among the most intrusive forms of monitoring. Current precedent still generally upholds video monitoring, but increasingly mentions the problematic nature of its invasiveness. It is only a matter of time before courts pressure employers to find other forms of less-intrusive monitoring. Therefore, a new monitoring regime should prohibit video surveillance of employees in private places where people are present<sup>257</sup> and limit video surveillance to Investigatory Purposes where: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Investigatory Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s).

The following figure classifies the top monitoring techniques into the four categories mentioned in Part IV. The Best Practices constitute low invasions of privacy and offer high enterprise protection for Business, Liability-Avoidance and Investigatory Purposes. Risky Practices move up the scale of invasiveness while continuing to provide employers with crucial benefits. Borderline Practices offer high enterprise protection while, at the same time, are highly invasive of employee privacy. Finally, Poor Practices generate high invasions of privacy and provide little enterprise protection for employers that cannot be obtained via less-invasive techniques. The American legal system is in this predicament due partially to the fact that evolving technology has caught Congress, state legislatures and the federal and state court systems off guard. Therefore, as the sliding scale moves up the invasiveness spectrum and

---

<sup>255</sup> *Id.* at 1082.

<sup>256</sup> *Id.*

<sup>257</sup> Under a new monitoring regime, a private place may be defined as any room or set of rooms in the workplace: (1) where employers allow or (2) where employees would reasonably expect that they are allowed to change clothes or otherwise tend to personal hygiene. The first part of the definition would give employers an opportunity to exclude personal offices or break rooms from the set of private places in their required notice. Employers would not, however, be allowed to exclude restrooms or locker rooms because any reasonable employee would believe that such places are private. Some courts do not currently require employer's conducting an investigation to use video surveillance in a narrowly tailored manner. *See Hillsides, supra* note 46, at 299 (discussing narrow tailoring and stating that contrary:

To what plaintiffs imply, it appears defendants are not required to prove that there were no less intrusive means of accomplishing the legitimate objectives we have identified above in order to defeat the instant privacy claim [based on the intrusion of the video surveillance]. In the past, we have specifically declined to “impos[e] on a private organization, acting in a situation involving decreased expectations of privacy, the burden of justifying its conduct as the ‘least offensive alternative’ possible under the circumstances.”)

The framework proposed in this article would require narrow tailoring because of the ever-increasing sophistication of contemporary video surveillance technology.

down the enterprise protection spectrum, a new monitoring regime must step in to rebalance the interests.

**Figure 4** - CLASSIFICATION OF THE TOP MONITORING TECHNIQUES

<b>CATEGORY I BEST PRACTICES</b> <input checked="" type="checkbox"/> LOW INVASIVENESS <input checked="" type="checkbox"/> HIGH PROTECTION <input checked="" type="checkbox"/> APPROPRIATE FOR ALL CATEGORIES	<b>CATEGORY II RISKY PRACTICES</b> <input checked="" type="checkbox"/> LOW INVASIVENESS <input checked="" type="checkbox"/> LOW PROTECTION <input checked="" type="checkbox"/> APPROPRIATE FOR LIABILITY-PREVENTION & INVESTIGATIONS <input checked="" type="checkbox"/> MUST PASS PJR FOR BUSINESS PURPOSES	<b>CATEGORY III BORDERLINE PRACTICES</b> <input checked="" type="checkbox"/> HIGH INVASIVENESS <input checked="" type="checkbox"/> HIGH PROTECTION <input checked="" type="checkbox"/> MUST PASS PJR FOR ALL MONITORING PURPOSES	<b>CATEGORY IV POOR PRACTICES</b> <input checked="" type="checkbox"/> HIGH INVASIVENESS <input checked="" type="checkbox"/> LOW PROTECTION <input checked="" type="checkbox"/> APPROPRIATE FOR INVESTIGATIONS ONLY IF IT PASSES PJR
ACCESS PANELS	FILTERS & FIREWALLS	E-MAIL & TEXT MESSAGE MONITORING	DESKTOP MONITORING
ATTENDANCE & TIME MONITORING	INTERNET & CLICKSTREAM DATA MONITORING	GPS & RFID MONITORING	KEYSTROKE MONITORING
AUTOMATIC SCREEN WARNINGS	SOCIAL NETWORK MONITORING	PHYSICAL SEARCHES	TELEPHONE & VOICEMAIL MONITORING
			VIDEO SURVEILLANCE

## VI. CONCLUSION

The twenty-first century continues to usher in new and increasingly-powerful technology. This technology is both a blessing and a curse in the employment arena. Sophisticated software and hardware allow businesses to conduct basic business transactions, avoid liability, conduct investigations and, ultimately, achieve success in a competitive global environment.<sup>258</sup> Employees can also benefit when monitoring provides immediate feedback, keeps the workforce efficient and focused and discourages unethical/illegal behavior. The same technology, however, allows employers to monitor every detail of their employees' actions, communications and whereabouts both inside and outside the

<sup>258</sup> Recall that employee activities are generally monitored for the following reasons:

1. To aid employers in conducting and completing business transactions (Business Purposes);
2. To aid employers in preventing civil lawsuits or criminal prosecutions (Liability-Avoidance Purposes);  
and
3. To aid employers conducting a pending internal or external investigation (Investigatory Purposes).

workplace. As more and more employers conduct some form of monitoring, the practice will shortly become ubiquitous. This trend is problematic because excessive and unreasonable monitoring can: (1) invade an employee's reasonable expectation of privacy, (2) lead employees to sneak around to conduct personal activities on work time, (3) lower morale, (4) cause employees to complain and, potentially, quit and (5) cause employees to fear using equipment even for benign work purposes.

Unfortunately, the American legal system has been slow to respond to the ever-increasing invasiveness and sophistication of contemporary monitoring technology. The most relevant federal law, the ECPA, was enacted over two decades ago and struggles to fit the square peg of 1980s "electronic communications" into the round hole comprised of the sophisticated monitoring techniques analyzed in Part III. In addition, the invasion of privacy torts (such as intrusion upon seclusion), offer little help to employees because of the decreased expectation of privacy inherent in any workplace. Finally, although many states have passed laws intended to protect employee privacy, this patchwork of state regulation is inconsistent and often pinpointed to single issues such as GPS tracking or e-mail monitoring. It is an easy case to make that the current legal regime is inadequate to protect an employee's every move from the scrutiny of today's monitoring practices.

The contemporary monitoring practices detailed in Part III, while all intrusive if abused, fall rather easily into four distinct categories - Best Practices, Risky Practices, Borderline Practices and Poor Practices. Each category dictates how the law should protect both employer and employee interests via an innovative sliding scale framework. The foundation of any new monitoring regime should require employers to provide advance notice of all monitoring practices and then cease and desist from certain practices depending upon the category under which the practice falls. The monitoring techniques classified as **Best Practices** should be allowed broadly for all three Monitoring Purposes (Business, Liability-Avoidance and Investigatory). The only restrictions on such monitoring occur when employers choose to implement a best practice outside of the three Monitoring Purposes. This would happen, for instance, if a supervisor chose to monitor and then complain about an employee's attendance records based on a personal grudge. The monitoring practices classified as **Risky Practices** are more privacy invasive than best practices. Therefore, a new legal regime should broadly allow this type of monitoring only for Liability-Prevention and Investigatory Purposes. When utilized for Business Purposes, these risky monitoring practices should be restricted to cases where an employer can articulate what this article styles the Privacy Judgment Rule (PJR). The PJR requires that: (1) the employer acts upon a reasonable business judgment that the monitoring is necessary for the specific Monitoring Purpose involved, (2) the monitoring is narrowly tailored (i.e., the least invasive method possible) to quickly and accurately discover the information at issue and (3) the monitoring targets only the relevant employee(s). However, while practices in the risky category are broadly allowed for Liability-Avoidance and Investigatory Purposes and limited to the PJR for Business Purposes, all **Borderline Practices** must meet the Privacy Judgment Rule. This increased scrutiny is merited because borderline practices are potentially more invasive than either best practices or risky practices. Finally, when dealing with **Poor Practices**, a new monitoring regime should: (1) prohibit poor practices from being utilized for Business and Liability-Avoidance Purposes and (2) limit poor practices during investigations where an employer can meet the Privacy Judgment Rule. The rationale behind this rather strict prohibition is that

the invasions that stem from poor monitoring practices are excessive and there are more effective, less-invasive ways for employers to protect the same interests.

The goal of this article is to contribute to the privacy literature in various ways. First, the discussion in Part II serves as a resource on how state and federal laws currently interact to “govern” employee monitoring. This data is currently spread far and wide throughout the legal, privacy and technology literature and online and the analysis in Part II attempts to capture a great deal of the data in one place. Second, this article is one of the few attempts in recent years to discuss the inner workings of contemporary monitoring technology as it relates to the law. Most articles on employee monitoring merely assert that “today’s monitoring technology is increasingly powerful and excessively dangerous” and move on to the legal analysis. This article explains how and why this technology can be dangerous before moving on to offer a solution. Finally, this discussion contributes another voice to the debate on how the American legal system must respond to contemporary employee monitoring - in this case arguing for a balanced monitoring framework that walks the fine line between creating efficient workplaces and avoiding excessive invasions of employee privacy. Whether such a regime is ultimately adopted by Congress (the preferred method) or various state legislatures is unclear. What is clear, however, is that without ripping apart the patchwork currently in place and starting over, this issue will continue to desperately seek a solution.