



TOURO UNIVERSITY
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 23 | Number 3

Article 6

May 2014

Webmail at Work: The Case for Protection Against Employer Monitoring

Marc A. Sherman

Follow this and additional works at: <https://digitalcommons.tourolaw.edu/lawreview>



Part of the [Communications Law Commons](#), and the [Computer Law Commons](#)

Recommended Citation

Sherman, Marc A. (2014) "Webmail at Work: The Case for Protection Against Employer Monitoring," *Touro Law Review*. Vol. 23: No. 3, Article 6.

Available at: <https://digitalcommons.tourolaw.edu/lawreview/vol23/iss3/6>

This Article is brought to you for free and open access by Digital Commons @ Touro Law Center. It has been accepted for inclusion in Touro Law Review by an authorized editor of Digital Commons @ Touro Law Center. For more information, please contact lross@tourolaw.edu.

WEBMAIL AT WORK: THE CASE FOR PROTECTION AGAINST EMPLOYER MONITORING

*Marc A. Sherman**

In the broad view, this Article is about privacy in the workplace—the rights and protections of employers and employees as to one another. Specifically, this Article addresses the issue of employer monitoring of employee email, with a focus on legal and ethical matters pertaining to web-based email (webmail).

The privacy issue is well settled when an employer monitors email sent through the company's own email system. Employers may unequivocally monitor any message that utilizes company-provided email. The law is not clear, however, when an employer accesses an employee's webmail. Neither statutes nor court decisions have addressed the privacy issues that arise when an employer monitors email sent by an employee via the employee's personal web-based email account.

The pervasiveness of email as a medium for both business and personal communications has resulted in a significant gap in privacy protection afforded to employees. Workers commonly use email for both business and personal purposes while at work. Yet, while the law safeguards workers' telephone conversations, postal mail, and personal space in the workplace, no protection currently exists for private webmail.

After revealing this webmail gap, the Article analyzes the business, public, and personal policy issues involved. These issues are cast in the broader context of privacy law and societal norms. Workplace behavior surveys are cited to establish the value and ex-

* J.D., Seton Hall University School of Law, 2007; B.G.S., International Economics, Ohio University, 1992. I wish to thank Professor Gaia Bernstein of Seton Hall University School of Law for her expert guidance and kind inspiration. Special thanks to my wife Orly for her unique insights and unwavering support.

pectations that employers and their workers each perceive in private communications. The Article then reveals how these values and expectations align with fundamental principals of privacy law.

The final analysis balances the legitimate business needs of employers to monitor email against the privacy needs of their workers. This Article concludes that workers' webmail should be protected by law. In the interim absence of such law, this Article sets forth policy suggestions for employers that take into account their legitimate business purposes for monitoring employee email as well as their employees' legitimate privacy concerns.

TABLE OF CONTENTS

INTRODUCTION	650
I. EMAIL USE IN THE WORKPLACE: A SURVEY OF AMERICAN BUSINESS CULTURE	654
II. WHY EMPLOYERS MONITOR EMAIL AND INTERNET USE	657
A. Reduce Risk of Legal Liability	657
B. Protect Assets	658
C. Prevent Loss of Productivity	659
III. HOW EMPLOYERS MONITOR EMAIL AND INTERNET USE	660
A. How Employers Monitor Email: A Technical Review ..	661
1. <i>On Email Servers</i>	661
2. <i>On PCs</i>	662
3. <i>On the Network</i>	663
B. How Employers Monitor Email: The Social Component	663
IV. LEGAL ANALYSIS: EMPLOYER MONITORING OF WORKERS' EMAIL IS LEGAL	664
A. Statutory Analysis	665

2007]	<i>WEBMAIL AT WORK</i>	649
	1. <i>The Electronic Communications Privacy Act</i>	665
	2. <i>The Stored Communications Act</i>	667
	B. Case Law—Intrusion upon Seclusion	668
	1. <i>Employees Have No Reasonable Expectation of Privacy</i>	668
	2. <i>Monitoring Is Not Highly Offensive</i>	670
V.	NORMATIVE ANALYSIS: WEBMAIL AT WORK SHOULD BE PROTECTED	675
VI.	POLICY SUGGESTIONS	679
VII.	CONCLUSION	682

WEBMAIL AT WORK: THE CASE FOR PROTECTION AGAINST EMPLOYER MONITORING

INTRODUCTION

“Why is beer better than women?”¹ Despite the inanity of this joke, it cost Chevron Oil Company \$2.2 million to settle a sexual harassment lawsuit.² The suit was brought by a group of employees alleging that Chevron allowed its internal email system to be used to disseminate sexually offensive content, including the sardonic account of the “25 Reasons Why Beer is Better than Women.”³

The *Chevron* settlement underscores one compelling reason for employers to monitor their employees’ email. The case settled in 1997—an evolutionary eon ago by internet standards.⁴ Since then, email has become a ubiquitous medium of communication among workers in businesses today. Its benefits are well known—email is easy to use, cheap, and fast. However, as email has proliferated, so

¹ JokesAndHumor.com, 25 Reasons Why Beer is Better than Women, <http://www.jokesandhumor.com/jokes/137.html> (last visited Sept. 10, 2007) (listing reasons such as “beer will always wait patiently for you in the car while you play baseball” and “[b]eer doesn’t demand equality”).

² See NANCY FLYNN, THE EPOLICY HANDBOOK 7 (2001).

³ *Id.*; Ann Carms, *Prying Times: Those Bawdy E-Mails Were Good for a Laugh -- Until the Ax Fell*, WALL ST. J., Feb. 4, 2000, at A1.

⁴ In January 1996, there were approximately 14.3 million hosts (computer systems with registered IP addresses). By January 2006, there were 395 million hosts. See Robert H. Zakon, Hobbes’ Internet Timeline v. 8.2, <http://www.zakon.org/robert/internet/timeline/#Growth>; see also Larry Irving, Assistant Sec’y for Commc’ns & Info., Nat’l Telecomms. & Info. Admin., U.S. Dep’t of Commerce, Remarks at the National Urban League & the National Leadership Council on Civil Rights Urban Technology Summit, Refocusing Our Youth: From High Tops to High-Tech (June 26, 1998), available at <http://www.ntia.doc.gov/ntiahome/speeches/urban62698.htm> (noting the growth in internet usage between 1996 and 1997 during which time the number of Fortune 500 Hundred companies with websites increased from thirty percent to eighty percent).

have the social and legal ramifications of its use and abuse. To the extent that employers embrace email for its benefits, so too are they wary of its risks. Liability for harassment, as in *Chevron*, is only one of the costly risks to which employers are exposed through widespread use of their email systems.⁵ A short list of other risks includes compromise of sensitive or proprietary information, damage to public image, and vicarious liability for various torts.

While it is accurate to describe email as a means to send and receive information instantly and cheaply, it is also true to think of it as a medium for the exchange of ideas. Email facilitates collaboration among workers in diverse locations by enabling them to express their thoughts virtually in real time. In these email discussions, raw information is merely a component. Often, the essence of such discussions consists of workers' thoughts and feelings on a subject. Information is not merely exchanged; it is developed. Even when used strictly for business purposes, therefore, email is a veritable window into the minds of its users—capturing, recording, and widely distributing their thoughts as written at a particular moment in time.

There is no controversy in this aspect of email. After all, workers comprehend the features of email that so readily memorialize their discussions. They use email *because* of these features—not in spite of them. When workers use email for personal communications, however, they hold no intention to share their thoughts with anyone other than to whom their messages are addressed. The fact

⁵ FLYNN, *supra* note 2, at 7-8, 61-62 (associating inappropriate email use with business risks such as compromised security, liability for software piracy, loss in productivity, and employee retention difficulties).

that email can be widely distributed or recorded does not mean that a worker wants an unintended audience. Yet, because email is prolific for personal as well as business correspondence, communication via employer-facilitated email is inevitable. This creates tension between the need for business to protect itself and the privacy interests of employees.

This Article analyzes the business interests of employers who monitor email and the privacy interests of their workers. Employers must protect themselves from the dangers of email misuse. To that end, many businesses monitor their employees' email to forestall delivery of inappropriate content or to mitigate damages by identifying employees who transgress. But to the extent that employees use email to express their thoughts, there is debate as to when and whether management may peruse their communications.

Generally, the law allows employers to monitor their workers' email.⁶ However, a distinction exists between employer-provided email ("work email") and web-based email ("webmail").⁷ Most case law on this issue addresses work email.⁸ Courts have universally held that employers' legitimate reasons for monitoring work email

⁶ It is a federal offense to "intentionally access without authorization a facility through which an electronic communication service is provided" except when applied "to conduct authorized . . . by the person or entity providing a wire or electronic communications service." 18 U.S.C.A. §§ 2701(a)(1), (c)(1) (2000). In the context of employment, the employer would be the provider of wire or electronic communication service. *See id.*

⁷ *See generally* SIMON GARFINKEL, WEB SECURITY, PRIVACY, AND COMMERCE 277 (2d ed. 2002).

⁸ *See* Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, at **1, 4 (D. Or. Sept. 15, 2004); Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *2 (D. Mass. May 7, 2002); Smyth v. Pillsbury Co., 914 F. Supp. 97, 98-99 (E.D. Pa. 1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *1 (Tex. App. May 28, 1999).

outweigh their workers' privacy interests—even when messages contain private information.⁹ But the law sheds little light on the subject of employer monitoring of workers' webmail, which by definition are private communications.

First, this Article describes the environment in which the debate arises. Surveys are used to illustrate the functions of email in today's business culture: how many workers use email at work, how often, and for what purposes. Next, this Article explains why employers monitor email; the dangers of email are real and substantial. Then, this Article explores the technical and social measures employers use to mitigate risk of email misuse. Next, this Article analyzes the law to the extent that it touches this issue and finds that the law clearly sanctions monitoring of work email, but that it is less clear with respect to webmail.

Further, in light of legitimate business exigencies, privacy law (as evolved in other contexts), and societal norms (vis-à-vis email communications inside and outside the workplace), employers should be allowed unfettered monitoring of email transmitted over their own email systems. However, the characteristics of webmail support a parallel conclusion that employers should not be permitted to monitor email communications when workers use their webmail. In the context of webmail, the interests of workers create a narrow zone of privacy into which employers may not intrude. Modern privacy law, as

⁹ See *Garrity*, 2002 WL 974676, at *2 (“Even if plaintiffs had a reasonable expectation of privacy in their work e-mail, defendant’s legitimate business interest in protecting its employees from harassment in the workplace would likely trump plaintiffs’ privacy interests.”)

it pertains to wiretapping, supports this notion.¹⁰ In addition, it conforms to the underlying policies of privacy law as embodied by the Constitution, the common law, and case law.

Finally, this Article suggests policies and practices that, in lieu of legislation, could enable employers to monitor workers' email in ways that achieve their security needs without alienating their employees.

I. EMAIL USE IN THE WORKPLACE: A SURVEY OF AMERICAN BUSINESS CULTURE

Work email utilizes an employer's own technological infrastructure. Email addresses for employees who have work email typically include some variation of their names followed by "@" followed by a variation of the employers' names. In addition to the email servers and connectivity that give email addresses existence and function, employers also provide the user interface software and equipment necessary for workers to use their email services. Employees usually access their email through an application such as Microsoft *Outlook* or IBM *Lotus Notes*.¹¹ Employees typically use

¹⁰ See Thomas R. Greenberg, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 246-47 (1994).

As a general premise, a court would allow any business-related communication to be monitored because it implicates the legal and legitimate business interests of the employer. By the same token, personal communications would be protected under Title III regardless of the circumstances, and could only be monitored to the extent necessary to determine that they are personal. Thus, under the subject matter approach, E-mail . . . should receive the same degree of protection as telephonic communications.

Id. at 246-47.

¹¹ See GARY B. SHELLY ET AL., *DISCOVERING COMPUTERS* 69 (4th ed. 2008); see also Charles Arthur, *Survival of the Unfittest*, *GUARDIAN* (London), Feb. 9, 2006, available at

email while at work on their employers' premises. However, those who work remotely (from home, hotels, etc.) can access work email through employer-provided virtual private networks.¹² This enables them to access their employers' secure, internal network as if they are virtually at the office.

Email has significant advantages over telephone communications—even conference calls. For instance, email discussions allow one to ponder and process a co-worker's message before responding. One may convey a message to multiple parties, thereby soliciting their participation—broadening a discussion and accelerating development of ideas.

Email constructs a record of discussions that can be stored indefinitely. This increases efficiencies by enabling workers to refer to previous discussions as needed. It provides accountability because workers' ideas, decisions, and actions are memorialized and easily retrievable. Also, storage of email discussions creates a virtual paper-trail of workers' activities—one that is ultimately at the sole disposal of their employers.

Internet access is also a common feature in the American workday. Many businesses utilize a private, secure *internal* network (intranet) to enable workers to access non-public information or use internal applications.¹³ But employees must often access *external*

<http://www.guardian.co.uk/technology/2006/feb/09/guardianweeklytechnologysection> (stating that IBM *Lotus Notes* is used by approximately 120 million people).

¹² See SHELLY, *supra* note 11, at 470. “[A] virtual private network . . . provides [mobile or remote users] with a secure connection to the company network server, as if [such users] had a private line. Virtual private networks help to ensure that transmitted data is safe from being intercepted by unauthorized people.” *Id.*

¹³ See *id.* at 307.

(internet) sites for business purposes as well. Such access can greatly increase the scope and volume of productivity by facilitating research and creativity.

More than 60 million Americans have email and/or internet access at work.¹⁴ Although email is an essential business tool, workers commonly use it for personal correspondence. As with work email, employees who have internet access at work frequently use it to exchange personal email via their webmail services. According to the ePolicy Institute, in 2004, eighty-six percent of workers who have work email and internet access use them for personal use.¹⁵ This includes shopping, corresponding with friends and family, browsing news, gossip, or personal interest sites, etc.¹⁶ In 2000, for example, nearly fifty percent of online holiday purchases were made during business hours.¹⁷ Another recent study revealed that eighty-three percent of the companies surveyed had employees who use webmail to send/receive email outside the business.¹⁸ Most workers use their webmail while at work for personal communications, just as they use work email to exchange thoughts on business and personal topics.¹⁹

¹⁴ Deborah Fallows, *Email at Work: Few Feel Overwhelmed and Most are Pleased with the Way Email Helps Them Do Their Jobs*, Pew Internet & American Life Project, Dec. 8, 2002, at 2, http://www.pewinternet.org/pdfs/PIP_Work_Email_Report.pdf.

¹⁵ Press Release, The ePolicy Institute, *2004 Survey on Workplace E-Mail and IM Reveals Unmanaged Risks*, <http://www.epolicyinstitute.com/survey/index.html> (last visited Oct. 24, 2007) [hereinafter E-Mail Survey].

¹⁶ See Douglas Schweitzer, *Workplace Web use: Give 'em an inch...*, SAPNEWS, Sep. 27, 2004, http://searchsap.techtarget.com/originalContent/0,289142,sid21_gci1009417,00.htm.

¹⁷ Russell J. McEwan & David Fish, *Privacy in the Workplace*, N.J. LAWYER, Feb. 2002, at 21.

¹⁸ RECONNEX 2005 INSIDER THREAT INDEX YEAR TO DATE FINDINGS 2 (2005), <http://weblog.infoworld.com/zeroday/archives/files/Reconnex%202005%20Insider%20Threat%20Findings.pdf>.

¹⁹ *Id.*

II. WHY EMPLOYERS MONITOR EMAIL AND INTERNET USE

It is necessary to understand the reasons why employers monitor their workers' email because, in actions for invasion of privacy, the courts often weigh these reasons against the privacy interests of employees.²⁰ Thus far, this calculus generally justifies email monitoring in the eyes of the courts.²¹

A. Reduce Risk of Legal Liability

The primary reason employers monitor email is to protect against legal liability for sexual harassment, hostile work environments, and fraud.²² Such liability can easily arise when employees exchange sexually explicit or otherwise offensive emails.²³ Employers risk liability even when inappropriate emails are exchanged among consenting co-workers.²⁴

²⁰ See Sindy J. Policy, *The Employer as Monitor: Keeping an Eye on Net Use and E-mails Can Prevent Litigation*, <http://abanet.org/buslaw/blt/ndpolicy.html> (last visited Sept. 10, 2007).

Potential lawsuits could allege a common law tort claim for invasion of privacy, or a statutory cause of action created by federal privacy statutes. However, courts have balanced the interests between employee privacy rights and employer rights to monitor Internet and e-mail use and held in favor of the employer's right to control its workplace.

Id.

²¹ See Kevin W. Chapman, Comment, *I Spy Something Read! Employer Monitoring of Personal Employee Webmail Accounts*, 5 N.C. J. L. & TECH. 121, 129 (2003).

²² See Micah Echols, *Striking a Balance Between Employer Business Interests and Employee Privacy: Using Respondeat Superior to Justify the Monitoring of Web-Based, Personal Electronic Mail Accounts of Employees in the Workplace*, 7 COMP. L. REV. & TECH. J. 273, 278 (2003); see also Erin M. Davis, Comment, *The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed by Their Employees*, 12 ALB. L.J. SCI. & TECH. 683, 688 (2002).

²³ See Policy, *supra* note 20.

²⁴ See Carrns, *supra* note 3 (explaining that The New York Times Company terminated nearly twenty employees for sending and/or receiving emails that included sexual images and offensive jokes).

According to a recent study, seventy percent of workers have admitted to viewing or sending sexually explicit email at work.²⁵ The threat this creates “continues to take a hefty toll on U.S. employers, with costly lawsuits—and employee terminations—topping the list of electronic risks. As recent court cases demonstrate, e-mail can sink businesses—legally and financially.”²⁶

B. Protect Assets

Protection of company assets ranks second among employers’ concerns.²⁷ Email poses a threat to a company’s information technology (“IT”) infrastructure by serving as a conduit for harmful programs.²⁸ When workers open attachments received from outside the company, visit insecure websites, or download files or programs from outside the corporate firewall, they pose a direct threat to employers’ networks, databases, servers, and workstations.²⁹ Although many companies go to great lengths to protect their IT assets from harmful intrusions, even companies that allocate large sums for the most comprehensive and advanced protection can only hope to keep up with the myriad permutations of viruses, worms, spy-ware and tro-

²⁵ Chapman, *supra* note 21, at 123.

²⁶ Press Release, American Mgmt. Assoc., 2006 Workplace E-Mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-Mail, IM & Blog Violators (July 11, 2006), available at http://www.amanet.org/press/amanews/2006/blogs_2006.htm [hereinafter Bosses Battle Risk].

²⁷ *Id.*

²⁸ See Chapman, *supra* note 21, at 123-24 (“[C]ompanies monitor e-mail usage to protect their assets. . . . [D]amage to computer resources via a virus are major concerns when employees use web-based e-mail programs.”). *Id.* at 124.

²⁹ See Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 121 (2005).

jans.³⁰

Email misuse can severely compromise a company's intangible assets, such as its intellectual property and public image.³¹ For instance, it takes a worker mere seconds to attach a document containing an employer's trade secret to an email and send it to a competitor. The same worker could just as easily broadcast a message that embarrasses his employer before clients, vendors, or the public.³²

C. Prevent Loss of Productivity

Finally, employers monitor email to guard against loss of productivity stemming from excessive non-business related activity.³³ For example, when one is browsing eBay in search of some obscure collectible, one is not performing the duties for which the employer pays. The cost to an employer of a worker spending five minutes to buy something online might seem negligible. But workers who use email and the internet at work to run side businesses, look for other jobs, or otherwise spend unduly long periods of time on non-business purposes present a clearer threat of productivity loss.³⁴ Employers, therefore, have clear, legitimate business purposes for monitoring

³⁰ See *The Evolution of Digital Rights Management and Its Role in Optimizing the Life Cycle of Software Products*, BUS. TRENDS Q., Q3 2006 ("[T]he threat landscape is increasingly being dominated by attacks and malicious code that are used to commit cybercrime."), available at <http://www.btquarterly.com/?mc=idcpanel-discusiion&page=sp-viewarticle>; see generally, Verizon, *Power of Two: Presence and Precision*, White Paper, WP11982 0906 (2006) (on file with author).

³¹ See Chapman, *supra* note 21, at 124.

³² See, e.g., *Booker v. GTE.net LLC*, 214 F. Supp. 2d 746 (E.D. Ky. 2002). In *Booker*, two Verizon employees created a "dummy" webmail account under the name of a co-worker and then used it to send a "rude" email to a customer. *Id.* at 748.

³³ See Chapman, *supra* note 21, at 121.

³⁴ *Id.*

employees' email.

Email monitoring is relatively cheap, simple to implement, and easy to operate.³⁵ Compared to telephone and video surveillance, email monitoring offers an extremely attractive cost-benefit. Employers who lack the funds or expertise to manage their own comprehensive email security apparatus can outsource some or all of it to a number of vendors. Given the low cost and ease of monitoring and the severity of the risks, email monitoring in the workplace is an established part of doing business. Fifty-five percent of United States employers monitor work email.³⁶ Employers are also concerned with inappropriate use of the internet, with seventy-six percent of United States employers monitoring their employees' web surfing.³⁷ Finally, thirty-six percent of employers monitor all activity on employees' computers through software that records keystrokes and screenshots.³⁸

III. HOW EMPLOYERS MONITOR EMAIL AND INTERNET USE

As a privacy issue, email monitoring in the workplace has two components: the technical apparatus that physically enables surveillance and the social practices designed to make it effective and, more importantly perhaps, legal.³⁹

³⁵ See Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-Mail and Internet Use*, July 9, 2001, <http://www.sonic.net/~undoc/extent.htm>. Email monitoring is largely automated, and thus it costs less than \$10.00 per employee, per year to operate. *Id.*

³⁶ AMERICAN MGMT ASS'N & THE ePOLICY INSTITUTE, 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY 1, 3 (2005) [hereinafter MONITORING SURVEY].

³⁷ *Id.* at 1.

³⁸ *Id.*

³⁹ Corey A. Ciocchetti, *Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 0026, ¶¶ 6-9 (2001),

A. How Employers Monitor Email: A Technical Review

Most companies deploy software and equipment to monitor activity on their networks.⁴⁰ It is feasible to monitor everything that takes place on an employer's network. Low-grade spy software is even available to average consumers—often marketed to jealous spouses and protective parents.⁴¹

Employers have unfettered access to inbound and outbound email that crosses their networks. Monitoring work email in particular is quite easy. But employers can also monitor workers' webmail and anything else done on their computers while on their employers' networks. This can be done at multiple levels: at the email level, on employees' computers, and on the network.

1. On Email Servers

Employers use software that automatically scans all inbound and outbound emails. Employers can configure the software to screen for specific content based on keywords, file types, file sizes, and parties involved. The information on these systems can be directly traced back to a named user. Every email that a worker sends can be actively read or passively monitored through keywords that

<http://www.law.duke.edu/journals/dltr/articles/2001dltr0026.html>.

⁴⁰ See MONITORING SURVEY, *supra* note 36, at 1.

⁴¹ See generally WebWatcher, <http://www.awarenesstech.com/cheating/?sid=30> (last visited Sept. 11, 2007). An example includes WebWatcher Computer Monitoring Software which says in its advertisement: "RECORD EVERYTHING that happens on any computer and see it online from anywhere." *Id.* See also Monitoring Software Reviews, <http://www.monitoringsoftwarereviews.org/> (last visited Sept. 11, 2007) ("[I]f you're looking to . . . keep an eye on a loved one, the software reviewed . . . on this site can help you do just that.").

alert administrators to look further into a particular user's behavior. Software can even distinguish between appropriate pictures and sexually explicit images.⁴²

2. *On PCs*

Employers may install software on workers' computers that records every keystroke and/or captures random images of what appears on employers' screens (screenshots). Such software can be installed and operated without a user's knowledge.⁴³ It captures screenshots at pre-set intervals and/or all text that an employee types by logging all keyboard inputs (key-logging). The software logs text even if an employee deletes it. For example, an employee might begin an angry response to a supervisor's email by typing: "I object to your instructions, you fool." After pausing to calm down, and having perhaps typed, "you fool" merely for cathartic purposes, the employee might use the backspace key to erase the last two words. The final email, therefore, would state: "I object to your instructions." However, because the key-logging software secretly captured the employee's keystrokes, the employer has a record of the employee's thoughts and feelings at that particular moment.

Web browsers record temporary files (log files with a history of visited sites) as well as "cookies" that record personal information

⁴² See, e.g., Verizon's Managed Email Content Service, which features image composition analysis technology to detect inappropriate images based on multiple image attributes (non-public product description, on file with author).

⁴³ For example, an employer can "push" (i.e., send) software through its network to all connected PCs. This can be done on an ad hoc basis, for individual users, or it can be done throughout an entire organization. Client Push Installation Properties, http://www.microsoft.com/technet/prodtechnol/sms/smsv4/smsv4_help/a8e6b23d-41aa-4971-bc47-c6c6184affe8.msp?mfr=true (last visited Sept. 10, 2007).

about the sites the user has visited. This information is stored on the computer and can be used to track where a user has been.

3. *On the Network*

It is more difficult for employers to monitor workers' webmail because the email servers through which it passes are not on their own network. However, employers can still monitor such emails by using a network "packet sniffer."⁴⁴ Such software resides on the network rather than on a worker's computer. As webmail messages travel back and forth over an employer's network, a sniffer captures the data packets and decodes and analyzes their content regardless of passwords or encryption.

B. **How Employers Monitor Email: The Social Component**

In conjunction with monitoring technology, employers also promulgate policies pertaining to email monitoring and provide notice to their workers that their email is subject to surveillance. To their credit, most employers who monitor their workers' email make concerted efforts to make their policies known to employees.⁴⁵ Such notifications typically appear in employee handbooks, at new-hire orientations, or through on-going corporate compliance trainings. These convey an implicit admonishment: workers are urged to modify their expectations of privacy accordingly. The following is a written policy as set forth in the employee handbook of Verizon, a major

⁴⁴ See KEVIN J. CONNOLLY, LAW OF INTERNET SECURITY AND PRIVACY 131 (2004 ed.).

⁴⁵ MONITORING SURVEY, *supra* note 36, at 1.

telecommunications corporation:

Electronic communications are considered to be Company property and are subject to inspection by the Company at any time without prior notice . . . Inappropriate use of these services is prohibited and may result in losing access and corrective action, up to and including termination of employment . . . Electronic Communications are considered to be the property of Verizon and the use of any such Electronic Communication services constitutes permission for Verizon to monitor communications on that service, including, but not limited to all electronic mail or any other electronic communication service, for any business purpose, including enforcement of this policy, or as required by law. Accordingly, in the course of their duties, system operators and managers may monitor use of the Internet or review the contents of transmitted data.⁴⁶

IV. LEGAL ANALYSIS: EMPLOYER MONITORING OF WORKERS' EMAIL IS LEGAL

There is no clear statutory prohibition of employer monitoring of email. Nor have courts discerned any meaningful privacy protections for employees from federal or state law. The law generally allows employers to monitor workers' private communications regardless of whether they take place over employer-provided email systems or web-based email, whether during business hours or after hours, and whether such communications take place in the office while physically on the employer's network or remotely such as accessing the network using encryption software.

⁴⁶ See Verizon Employee Handbook (2006) (non-public document, on file with author).

A. Statutory Analysis

1. *The Electronic Communications Privacy Act*

The Electronic Communications Privacy Act⁴⁷ (“ECPA”) prohibits interception of email.⁴⁸ It applies to “any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept . . . any . . . electronic communication”⁴⁹ But while the ECPA proscribes a broad scope of electronic eavesdropping, it is generally inapplicable to email monitoring in the workplace and employees can expect little protection from it in this context.

To “intercept” a communication, one must acquire it during transmission. The act of *accessing* communications that have arrived at any destination, such as an email server, is not within the ambit of the ECPA.⁵⁰ Work email reaches the employer’s server almost instantaneously after transmission, so there is no liability for interception, as proscribed by the statute.⁵¹ Webmail, on the other hand, does not touch an employer’s server. Rather, it merely traverses the employer’s network to/from the webmail provider’s server. Therefore, webmail monitoring, arguably, does not fall within the definition of “interception” under the ECPA.

If an employee complainant overcomes the interception-

⁴⁷ 18 U.S.C.A. §§ 2510-2521 (West 2000).

⁴⁸ *Id.* § 2511(1)(a).

⁴⁹ *Id.*

⁵⁰ *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635, 636 (E.D. Pa. 2001); *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. 2002).

⁵¹ *Garrity*, 2002 WL 974676, at *3 (noting that where defendant employer accessed plaintiff employee’s email after it was sent, “the act of ‘interception’ cannot proceed after the e-mail is received”).

access dichotomy, he still faces two powerful exceptions that make the ECPA inapplicable to workplace email surveillance. First, the statute allows surveillance if the parties involved consent.⁵² This exception relieves employers of liability under the ECPA when, as many do, they emphatically put their employees on notice that their email can and shall be monitored. Many employers obtain express consent by requiring their workers to sign forms that specifically set forth email monitoring policies. Even without consent forms, consent may very well be implied courts when such policies are nonetheless promulgated in employee handbooks.⁵³ Since eighty-six percent of businesses that monitor email inform their employees of their policies, the consent exception usually applies.⁵⁴

Secondly, since employers are the providers of the service and technical infrastructure over which employees' email passes, the ECPA does not apply to employers because of the "provider exception," which states:

It shall not be unlawful . . . [for] a provider of wire or electronic communications service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of

⁵² 18 U.S.C.A. § 2511(2)(c) (West 2000).

⁵³ See *Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746, at *20 (D. Or. 2004) ("[Plaintiff] may not have had a reasonable expectation of privacy in his personal [email] folders simply because of the explicit policies set out in [defendant's] Employee Handbook.").

⁵⁴ MONITORING SURVEY, *supra* note 36, at 2.

that service⁵⁵

Employers are invariably the service providers within the context of the ECPA, as they provide the computers, connectivity, and IP addresses that employees require to do their jobs.⁵⁶

In summary, an employer can avoid liability under the ECPA if: (1) it monitors email only after it reaches the email server; (2) it provides notice (express or implied) to employees that their emails may be monitored; and (3) it provides the facilities employees use to send/receive email.⁵⁷ Not surprisingly, courts have overwhelmingly ruled in favor of employers in actions brought by employees under the ECPA.⁵⁸

2. *The Stored Communications Act*

While employers might not be liable under the ECPA because email monitoring does not fall within the definition of *interception*, the Stored Communications Act (“SCA”) prohibits unauthorized access to *stored* electronic communications.⁵⁹ The SCA provides for a private cause of action for unauthorized access to stored data, such as found on a computer’s hard drive or email servers.⁶⁰

⁵⁵ 18 U.S.C.A. § 2511(2)(a)(i) (West Supp. 2007).

⁵⁶ TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 164 n.10 (Cal. Ct. App. 2002) (noting that even if an employee uses company-provided equipment at home, “in ‘today’s portable society, where one’s computer files can be held and transported in the palm of the hand, relevant evidence should not escape detection solely because it was created within the physical confines of one’s home.’ ”).

⁵⁷ See *id.* at 162-64; *Fraser*, 135 F. Supp. 2d at 636.

⁵⁸ Christopher Pearson Fazekas, *1984 is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law*, 2004 DUKE L. & TECH. REV. 15 ¶¶ 5, 6 (2004).

⁵⁹ 18 U.S.C.A. § 2701(a) (West 2000).

⁶⁰ *Id.* § 2707(a) (West Supp. 2007).

Nevertheless, employers are rarely liable under the SCA because this statute also contains a “provider exception.”⁶¹ Furthermore, an employer does not violate the SCA if it has legitimate business purposes for accessing employees’ stored emails.⁶² In actions brought against employers by workers under the SCA, as with those brought under the ECPA, courts almost always find in favor of the employer.⁶³

B. Case Law—Intrusion upon Seclusion

Employees who object to having their personal email monitored at work have a more plausible cause of action for intrusion upon seclusion.⁶⁴ This requires an employee to show that there was a reasonable expectation of privacy and that the employer’s act constituted a highly offensive intrusion.⁶⁵

1. *Employees Have No Reasonable Expectation of Privacy*

The ECPA embraces Justice Harlan’s concurring opinion in *Katz v. United States*,⁶⁶ in which the Supreme Court supported the principle that Fourth Amendment privacy protection applies to people

⁶¹ *Id.* § 2701(c)(1) (stating that the person or entity which provides the communication service is excluded under the SCA).

⁶² *Id.* § 2701(c)(2).

⁶³ See Fazekas, *supra* note 58, ¶ 6.

⁶⁴ See *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (noting that electronic intrusion into a private place may violate the Fourth Amendment.)

⁶⁵ See *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611, 621 (3rd Cir. 1992) (finding that liability for intrusion applies when the intrusion “would be highly offensive to ‘the ordinary reasonable person’ ” (citation omitted)).

⁶⁶ 389 U.S. 347 (1967).

who have a reasonable expectation of privacy.⁶⁷ The *Katz* Court determined that a person must have an expectation of privacy that “society is prepared to recognize as ‘reasonable.’”⁶⁸ The ECPA codifies this requirement by prohibiting surveillance of communications in situations where a person manifests “an expectation that such communication is not subject to interception under circumstances justifying such expectation”⁶⁹

In the context of employer surveillance of email, however, courts have ruled that employees have little or no “reasonable expectation of privacy in the contents of the[ir] email.”⁷⁰ In *Smyth v. Pillsbury Co.*,⁷¹ the employer assured employees that “all e-mail communications would remain confidential and privileged.”⁷² Even so, an action for intrusion upon seclusion failed for lack of expectation of privacy.⁷³

Applying the Restatement definition of the tort of intrusion upon seclusion to the facts and circumstances of the case . . . we find that plaintiff has failed to state a claim upon which relief can be granted. . . . [W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system *notwithstanding any assurances that such communications would not be intercepted by management*. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an

⁶⁷ *Id.* at 353.

⁶⁸ *Id.* at 361.

⁶⁹ 18 U.S.C.A. § 2510(2).

⁷⁰ *See, e.g., McLaren*, 1999 WL 339015, at *4.

⁷¹ 914 F. Supp. 97 (applying reasoning similar to that applied in *McLaren*).

⁷² *Id.* at 98.

⁷³ *Id.* at 100-01.

e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.⁷⁴

2. *Monitoring Is Not Highly Offensive*

Under the Restatement (Second) of Torts, “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”⁷⁵ Actions for intrusion upon seclusion have also failed because courts do not consider email monitoring to be an invasion of privacy that is highly offensive to the reasonable person.⁷⁶ The analysis is largely based on the relative values of business interests and employee privacy interests.⁷⁷

In *McLaren v. Microsoft Corp.*,⁷⁸ an employee claimed that Microsoft invaded his privacy by accessing email stored in his personal folders on his computer at work.⁷⁹ Citing *Smyth*, the *McLaren* court held that “a reasonable person would not consider Microsoft’s interception of these communications to be a highly offensive invasion.”⁸⁰ In particular, the court noted that “the company’s interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh McLaren’s

⁷⁴ *Id.* (emphasis added).

⁷⁵ RESTATEMENT (SECOND) OF TORTS § 652B (1977).

⁷⁶ *E.g., Borse*, 963 F. Supp. at 621.

⁷⁷ *See Smyth*, 914 F. Supp. at 100.

⁷⁸ No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. 1999).

⁷⁹ *Id.* at *1.

⁸⁰ *Id.* at *5.

claimed privacy interest in those communications.”⁸¹

The legitimate business interest threshold is easy to meet when work email is the subject of monitoring. After all, work email itself is the employer’s property. But the issue of employer monitoring of webmail (which belongs to the user and merely utilizes the employer’s internet access) is less clear. As webmail passes through a technical infrastructure provided, paid for, maintained by, and under the control of the employer, the employers’ rationale for webmail monitoring would be that all information that passes through their facilities is company property and is subject to their full control.⁸² Since webmail poses many of the same risks as work email, the legitimate business reasons for monitoring it are comparable to those for monitoring work email. But employees’ privacy interests in webmail are not necessarily comparable. Whereas the law appears clear with regard to work email monitoring, case law and privacy law in general do not readily support webmail monitoring.

In *Fischer v. Mt. Olive Lutheran Church, Inc.*,⁸³ the defendant employed a crude, unsophisticated means to access the plaintiff’s Hotmail account: defendant sat at plaintiff’s computer and simply guessed his password.⁸⁴ Far from the impersonal and transparent monitoring that employers typically utilize, the defendant’s act actually involved physical access to plaintiff’s real space.⁸⁵ The court denied the defendant’s motion for summary judgment despite con-

⁸¹ *Id.*

⁸² See 18 U.S.C.A. § 2511(2)(a)(i) (West 2007).

⁸³ 207 F. Supp. 2d 914 (W.D. Wis. 2002).

⁸⁴ *Id.* at 920.

⁸⁵ *Id.* at 925.

trolling authority to the contrary,⁸⁶ as set forth in *Hillman v. Columbia County*.⁸⁷ In *Hillman*, the court gave undue attention to the meaning of “place” under the Wisconsin statute at issue.⁸⁸ According to the statute, intrusion upon seclusion occurs “in a place that a reasonable person would consider private”⁸⁹ The *Hillman* court was unable to reconcile the presence of the word “place” with the language in the Restatement (Second) of Torts.⁹⁰ The court reasoned, without examining the statute’s legislative history, that the legislature purposefully drafted language differently than the Restatement.⁹¹ In furtherance of its plain-meaning analysis, the *Hillman* court then cited a dictionary to support its conclusion that “the plain meaning of a ‘place’ is geographical.”⁹²

However, the *Fischer* court understood that, under the same statute, the word “place . . . does not limit the intrusion to a person’s immediate physical environment”⁹³ Moreover, the court stated that the issue should be interpreted in accordance with the Restatement.⁹⁴ Despite *Hillman*’s controlling authority, the *Fischer* court boldly determined that “it is disputed whether accessing plaintiff’s email account is highly offensive to a reasonable person and whether plaintiff’s email account is a *place* that a reasonable person would

⁸⁶ *Id.* at 930-31.

⁸⁷ 474 N.W.2d 913 (Wis. Ct. App. 1991).

⁸⁸ WIS. STAT. § 995.50(2)(a) (2006).

⁸⁹ *Id.*

⁹⁰ *Hillman*, 474 N.W.2d at 919 n.8.

⁹¹ *Id.* at 919.

⁹² *Id.*

⁹³ *Fischer*, 207 F. Supp. 2d at 928.

⁹⁴ *Id.*

consider private”⁹⁵ The presence of the word “place” in the statute is merely semantic and not substantive, as summarily determined in *Hillman*.⁹⁶ Casting doubt on the *Hillman* court’s reasoning, the *Fischer* court denied defendant’s motion for summary judgment, and in so doing, kept the notion of intrusion upon seclusion in cases involving webmail in the workplace viable.⁹⁷

Another important case that deals with employer monitoring of webmail is *Booker v. GTE.net LLC*.⁹⁸ This case also provides little guidance as to intrusion upon seclusion in employer monitoring of webmail. However, it is instructive as to the personal nature of webmail. In *Booker*, two Verizon employees created a “dummy” webmail account under Booker’s name.⁹⁹ Falsely portraying themselves as Booker, a putative customer service representative, they used the account to send a “rude” and embarrassing email to a Verizon customer.¹⁰⁰ Booker’s management initially blamed her for the email.¹⁰¹ Verizon interrogated her and soon understood that she was not the author.¹⁰² After the investigation, Booker sued the company for emotional and psychological injuries on a theory of vicarious li-

⁹⁵ *Id.* (emphasis added).

⁹⁶ See Lisa Infield-Harm, Note, *The Case for Reexamining Privacy Law in Wisconsin: Why Wisconsin Courts Should Adopt the Interpretation of the Tort of Intrusion Upon Seclusion of Fischer v. Mount Olive Lutheran Church*, 2004 WIS. L. REV. 1781 (2004) (“In *Hillman*, the Wisconsin Court of Appeals rejected a common sense approach to the tort of intrusion upon seclusion, and instead created an arguably flawed threshold question for the tort - whether the defendant invaded a ‘place’ within the meaning of [the statute]”). *Id.* at 1782.

⁹⁷ *Fischer*, 207 F. Supp. 2d at 928.

⁹⁸ 214 F. Supp. 2d 746 (E.D. Ky. 2002).

⁹⁹ *Id.* at 748.

¹⁰⁰ *Id.* at 747-48.

¹⁰¹ *Id.* at 747.

¹⁰² *Id.* at 748.

ability.¹⁰³ Her claim failed because she was unable to show that the tortfeasors committed their act within the scope of their employment.¹⁰⁴ Pursuant to Kentucky law, the court considered:

(1) whether the conduct was similar to that which the employee was hired to perform; (2) whether the action occurred substantially within the authorized spacial and temporal limits of the employment; (3) whether the action was in furtherance of the employer's business; and (4) whether the conduct, though unauthorized, was expectable in view of the employee's duties.¹⁰⁵

The court analyzed these four prongs and found that the acts were indeed similar to the tortfeasors' legitimate duties and that they were undoubtedly committed in the workplace.¹⁰⁶ However, the court also determined that the act was not meant to further Verizon's business.¹⁰⁷ To the contrary, it was harmful to the company, as the tortfeasors instructed Verizon's customer to switch to a competitor.¹⁰⁸ Finally, the court concluded that it is axiomatic that Verizon does not expect such conduct from its customer service employees.¹⁰⁹

Booker draws a dim line between webmail and work email. Although the employees' actions involved webmail use on the employer's premises and during business hours, it was sufficiently distinct from work email so its effects were not imputed to the employer

¹⁰³ *Booker*, 214 F. Supp. 2d at 748.

¹⁰⁴ *Id.* at 751.

¹⁰⁵ *Id.* at 749.

¹⁰⁶ *Id.* at 750.

¹⁰⁷ *Id.*

¹⁰⁸ *Booker*, 214 F. Supp. 2d at 750.

¹⁰⁹ *Id.*

for purposes of vicarious liability.¹¹⁰ This delineation suggests the presence of boundaries between webmail and work email and, furthermore, that the boundaries influence the rights of employers and employees. *Booker* faintly supports the notion that employers do not have the same *carte blanche* rights to monitor webmail as they do work email.¹¹¹

V. NORMATIVE ANALYSIS: WEBMAIL AT WORK SHOULD BE PROTECTED

The common law of torts provides individuals with the right to sue when one intrudes upon their seclusion or solitude in a manner that is “highly offensive to a reasonable person.”¹¹² Similarly, one must have an objectively reasonable expectation of privacy.¹¹³ But what is reasonable when it comes to webmail? There are no statutory indicia and the sparse case law dealing with webmail monitoring provides little comment. Despite the dearth of legal authority on the subject, a strong argument arises in favor of webmail privacy in the workplace by examining general attitudes, policies, and laws concerning privacy.¹¹⁴

The United States Constitution, federal and state laws, and case law form a patchwork of privacy protections. Rather than a broad, overarching privacy law, as found in most other industrialized

¹¹⁰ *See id.* at 751.

¹¹¹ *See id.*

¹¹² RESTATEMENT (SECOND) OF TORTS § 652B (1977).

¹¹³ *Katz*, 389 U.S. at 361.

¹¹⁴ *See Hornung, supra* note 29, at 116.

nations, American privacy law is excessively particular.¹¹⁵ This is thought to be a weakness,¹¹⁶ but this structure draws an interesting picture of American values as they pertain to privacy interests. For example, privacy law protects people's records of video rental purchases. Congress passed the Video Privacy Protection Act in the wake of the controversy that arose when Judge Robert Bork's video rental records were published during his Supreme Court confirmation hearings.¹¹⁷ The murder of actress Rebecca Schaeffer, whose killer found her address through the Department of Motor Vehicles, led to the Drivers Privacy Protection Act.¹¹⁸ The Children's Online Privacy Protection Act protects children under the age of 13 on the internet.¹¹⁹ In addition to these federal laws, there is an abundant body of state law.¹²⁰ These and a plethora of other precisely targeted privacy laws indicate the degree to which Americans value privacy of personal information and the contexts in which privacy issues are likely to arise.

In the context of intrusion upon seclusion, this is important because it militates strongly in favor of the argument that unauthorized access to personal information is highly offensive to the reasonable person. This attitude prevails whether such intrusion is commit-

¹¹⁵ See generally JAY STANLEY & BARRY STEINHARDT, BIGGER MONSTER, WEAKER CHAINS: THE GROWTH OF AN AMERICAN SURVEILLANCE SOCIETY 15 (ACLU: Technology and Liberty Program, 2003), http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf.

¹¹⁶ See *id.* (noting that the European Union ranks United States data-protection policies at a level comparable to Third World countries).

¹¹⁷ See 18 U.S.C.A. § 2710(b)(1) (West 2000).

¹¹⁸ See *id.* §§ 2721(a)-(b) (West 2000).

¹¹⁹ See 15 U.S.C.A. § 6502 (West Supp. 2007).

¹²⁰ See, e.g., N.Y. PENAL LAW § 250.25 (McKinney 2007); see also OR. REV. STAT. ANN. § 164.162 (West 2007).

ted by the government or a private entity.¹²¹ There is widespread ignorance of general business practices that threaten privacy.¹²² But that does not necessarily translate into apathy.¹²³ Americans want their privacy and they expect it—often times even when it has already been compromised.¹²⁴ Conversely, when it comes to email monitoring in particular, employees are in the know, since nearly eighty percent of businesses explicitly notifying employees that their email may be under surveillance.¹²⁵ Among these employees, many perceive email monitoring as a threat to their privacy.¹²⁶ Despite such widespread awareness and concern, however, workers continue to exchange personal email while at work.¹²⁷ This further underscores the normative function of email as a diffuse tool for personal communication whether or not one is at work.

While the law accords due protection in comparable circumstances, it is curiously indifferent about email privacy. The ECPA

¹²¹ ELECTRONIC PRIVACY INFORMATION CENTER, PUBLIC OPINION ON PRIVACY, <http://www.epic.org/privacy/survey/> (last visited Sept. 10, 2007). A Gallup Poll published in May 2006 revealed that 62 percent of those surveyed “favored immediate Congressional hearings . . .” to investigate the recently exposed National Security Agency practice of keeping records of phone calls of millions of Americans. *Id.* at 7, 8. A poll published in the Washington Post in January 2006 showed that 64 percent of those surveyed “believed that federal agencies were intruding on Americans’ privacy rights in investigating terrorism.” *Id.* at 8.

¹²² See JOSEPH TUROW, LAUREN FELDMAN & KIMBERLY MELTZER, ANNENBERG PUBLIC POLICY CENTER OF THE UNIVERSITY OF PENNSYLVANIA, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 3 (2005).

¹²³ See PUBLIC OPINION ON PRIVACY, *supra* note 121, at 1; *but see* TUROW ET AL., *supra* note 122, at 3-4.

¹²⁴ See PUBLIC OPINION ON PRIVACY, *supra* note 121, at 1.

¹²⁵ See *Bosses Battle Risk*, *supra* note 26.

¹²⁶ See Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241, 242 (2006); *see also* Gaia Bernstein, *When New Technologies are Still New: Windows of Opportunity for Privacy Protection*, 51 VILL. L. REV. 921, 925 (2006).

¹²⁷ See *E-Mail Survey*, *supra* note 15.

protects against employer monitoring of employee phone calls;¹²⁸ monitoring only being allowed if an employee consents or if monitoring is conducted in the ordinary course of business.¹²⁹ Although these requirements are similar to those employers face for email monitoring under the ECPA, the courts have construed the statute far more strictly (i.e., in favor of privacy rights) in the context of telephone monitoring.¹³⁰ Stricter still is the protection of postal mail.¹³¹ Federal law has made it a criminal offense to open another's mail.¹³² Courts have even found intrusion upon seclusion when an employer reads an employee's private mail.¹³³ But "[t]he law has endorsed the broad monitoring of email and [i]nternet use by employers and in effect pronounced that such actions are not illegal."¹³⁴

Does the law accurately represent the underlying values of privacy interests? Or is it simply not sufficiently evolved to embody electronic privacy in the workplace? As discussed, privacy law in the U.S. is reactionary—statutes and court decisions often promulgated in response to a realized threat, rather than the core issues therein.¹³⁵ “The key to understanding legal privacy as it has developed over 100 years of American life, it will be argued, is to understand that its meaning is heavily driven by the events of history.”¹³⁶ If so, then the

¹²⁸ See generally 18 U.S.C.A. §§ 2510-21 (West 2000).

¹²⁹ See *id.* §§ 2510(5)(a)(i), 2511(2)(d) (West 2000).

¹³⁰ See *id.* §§ 2510(1), (5) (West 2000 & West Supp. 2007).

¹³¹ See *id.* § 1708 (West 2000).

¹³² See *id.* § 1702.

¹³³ See *Vernars v. Young*, 539 F.2d 966, 969 (3d Cir. 1976).

¹³⁴ Bernstein, *The Paradoxes of Technological Diffusion*, *supra* note 126, at 277.

¹³⁵ See Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340 (1992).

¹³⁶ *Id.*

2007]

WEBMAIL AT WORK

679

day will come when the law will align with both business needs to monitor employees and societal norms, behaviors, and expectations pertaining to personal privacy. In 1928, the Supreme Court declared “[t]he reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment.”¹³⁷ Forty years later, the Court reversed, holding:

The Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.¹³⁸

VI. POLICY SUGGESTIONS

Webmail lies within a narrow zone of privacy to which employers are not privy. Workers do not receive computers and network connectivity as luxuries. Rather, businesses deploy them as essential tools that workers must use in performance of their duties. Among these technological resources are telephones and email—communication pathways used prolifically for personal as well as business correspondence. Most employers accept the reality that workers will inevitably make personal phone calls during the eight

¹³⁷ *Olmstead v. United States*, 277 U.S. 438, 466 (1928).

¹³⁸ *Katz*, 389 U.S. at 353.

hours they are in their offices. It is natural that while spending one third of a day working, an employee may need to speak with a spouse, doctor, child's teacher, etc. Similarly, the realities of the modern work day compel workers to use webmail for non-business purposes. It follows that society accepts personal webmail communication to the extent that email has supplanted the telephone as a communications medium by today's workers.

Rather than wait for the law to establish boundaries, businesses might readily take the lead through self-regulation if the cost-benefit analysis so dictates. One compelling benefit of curtailing employee surveillance in general is improved morale among workers.¹³⁹

For employees who leave the house before dawn and don't return until well past dark, eMail may be the most efficient and effective way to stay in touch with family members. For the sake of employee morale and retention, savvy employers generally are willing to accommodate their employees' need to check in electronically with children and spouses.¹⁴⁰

Employers face daunting costs when peeved workers are provoked to leave.¹⁴¹ Particularly in competitive job markets when busi-

¹³⁹ See Personneltoday.com, PC Monitoring Could Damage Worker Morale, <http://www.personneltoday.com/Articles/2006/01/24/33534/pc-monitoring-could-damage-worker-morale.html> (last visited Sept. 10, 2007).

¹⁴⁰ See FLYNN, *supra* note 2, at 203.

¹⁴¹ For example, one commentator notes that "[i]t costs you 30-50% of the annual salary of entry-level employees, 150% of middle level employees, and up to 400% for specialized, high level employees!" Ross Blake, *Employee Retention: What Employee Turnover Really Costs Your Company*, WEBPRONEWS, July 24, 2006, <http://www.webproneWS.com/expertarticles/expertarticles/wpn-62-20060724EmployeeRetentionWhatEmployeeTurnoverReallyCostsYourCompany.html>.

nesses are most susceptible to high turnover, employers should balance security needs and the extent to which they monitor with the potential for perceived oppression among employees. It is not sufficient to notify workers that they are being watched. As discussed, such warnings do not obviate the reasonable needs of workers to communicate, nor do they influence their behavior. The effect of comprehensive monitoring is simply to alienate workers from their employers.

Employers can avoid scaring their workers and still manage the risks of non-business data flowing through their networks by incorporating normative realities into their policies. Employers should try to gain worker “buy-in” to the greatest extent possible. Rather than merely notifying workers of the surveillance, employers should explain the reasons behind it. If workers are educated about the legitimate risks as well as the protective measures, they are more likely to empathize with their employers’ policies than feel oppressed by them. Employers’ policies should also explicitly allow limited use of webmail. “American workers today put in more on-the-job hours than at any time in history. . . . [Employers should let] employees know where [they] stand on [the] issue [of personal email monitoring], and how much personal use (if any) is acceptable.”¹⁴²

Finally, if a company absolutely must prevent all use of webmail, its surveillance practices should specifically embody webmail at both the social and technical levels. The word “webmail” should appear in the company’s written policies. Additionally, employers

¹⁴² See FLYNN, *supra* note 2, at 203.

should implement network controls to physically bar access to as many webmail sites as possible. Some sources suggest that 65 percent of companies already block access to internet sites they consider to be inappropriate.¹⁴³ Such precautions are unlikely to forestall access to all webmail sites, but they can attenuate webmail use significantly by targeting popular webmail services, such as AOL, Gmail, and Hotmail. When access to an unblocked webmail site is detected, the employer should dispense discipline based only on the knowledge that a worker has accessed webmail. If the employer's policy is clear and well-disseminated, knowledge that an employee has used webmail is sufficient for the employer to protect itself while not violating the employee's privacy interests by actually reading it.

VII. CONCLUSION

"Everything that is really great and inspiring is created by the individual who can labor in freedom."¹⁴⁴ This bit of wisdom comes from Albert Einstein, a humble man always wary of authority.¹⁴⁵ One wonders where this idea belongs in the various management styles throughout American business. The Chevrons of the world are understandably reticent about the notion that employees should enjoy the freedom of private email at work. For corporate leaders accountable to shareholders, multi-million dollar lawsuits are powerful

¹⁴³ Amy B. Crane, Workplace Privacy? Forget It!, WORKRIGHTS.ORG, July 18, 2005, http://www.workrights.org/in_the_news/in_the_news_bankrate.html.

¹⁴⁴ ALBERT EINSTEIN, OUT OF MY LATER YEARS 19 (1950).

¹⁴⁵ Tony Phillips, Was Einstein a Space Alien?, SCIENCE@NASA, Mar. 23, 2005, http://science.nasa.gov/headlines/y2005/23mar_spacealien.htm ("Einstein didn't give a fig for authority. He didn't resist being told what to *do*, not so much, but he hated being told what was *true*.").

2007]

WEBMAIL AT WORK

683

precedents to heed. And it's not only shareholders and officers who derive the perceived benefits of caution. Workers themselves benefit as well, to the extent that their fortunes align with those of their employers.

But there is an opportunity cost which, though more difficult to perceive, is dangerously high. It arises from the types of opportunities and benefits not realized in environments that stifle free thought. Albert Einstein is an example of what one can achieve without the presence of undue control. Managers today are familiar with the concept of opportunity cost. They should observe a boundary in workplace surveillance that bars webmail monitoring—knowing that the opportunity cost of crossing this boundary makes webmail monitoring economically unwise as well as socially unnatural.

