March, 2007

Webmail at Work: The Case for Protection Against Employer Monitoring

Marc A Sherman, Seton Hall University School of Law

Available at: https://works.bepress.com/marc_sherman/1/
WEBMAIL AT WORK:
THE CASE FOR PROTECTION AGAINST EMPLOYER MONITORING

Marc A. Sherman

March 30, 2007

INTRODUCTION................................................................................................................................1
I. EMAIL USE IN THE WORKPLACE: A SURVEY OF AMERICAN BUSINESS CULTURE. ................... 4
II. WHY EMPLOYERS MONITOR EMAIL AND INTERNET USE......................................................... 6
   A. Reduce Risk of Legal Liability........................................................................................... 6
   B. Protect Assets...................................................................................................................... 7
   C. Prevent Loss of Productivity ............................................................................................. 8
III. HOW EMPLOYERS MONITOR EMAIL AND INTERNET USE. .................................................... 9
   A. How Employers Monitor Email: A Technical Review....................................................... 9
      1. On Email Servers ............................................................................................................ 9
      2. On PCs .......................................................................................................................... 10
      3. On the Network ............................................................................................................. 10
   B. How Employers Monitor Email: The Social Component................................................. 11
IV. LEGAL ANALYSIS: EMPLOYER MONITORING OF WORKERS’ EMAIL IS LEGAL. .................. 12
   A. Statutory Analysis............................................................................................................. 12
      1. The Electronic Communications Privacy Act............................................................... 12
      2. The Stored Communications Act .................................................................................. 14
   B. Case Law – Intrusion upon Seclusion ............................................................................ 15
      1. Employees Have No Reasonable Expectation of Privacy ............................................ 15
      2. Monitoring Is Not Highly Offensive............................................................................. 16
V. NORMATIVE ANALYSIS: WEBMAIL AT WORK SHOULD BE PROTECTED. ......................... 20
VI. POLICY SUGGESTIONS........................................................................................................... 23
CONCLUSION.................................................................................................................................. 25
INTRODUCTION

“Why is beer better than women?” Despite the inanity of this joke, it cost Chevron Oil Company $2.2 million to settle a sexual harassment lawsuit. 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.”

_Chevron_ underscores one compelling reason for employers to monitor their employees’ email. The case settled in 1997 – an evolutionary eon ago by internet standards. 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. But as email has proliferated, so 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. 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 disparately located workers 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; rather, it is developed. Even when used strictly for business purposes, therefore, email is a veritable window into the minds of its users – capturing, widely distributing, and recording 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 those to whom their messages are addressed. The fact that email can be widely distributed or recorded does not mean that a worker wants an unintended audience. Yet, because email is as 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 paper 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 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. However, a distinction exists between employer-provided email (“work email”) and web-based email
Most case law on this issue addresses work email. Courts have universally held that employers’ legitimate reasons for monitoring work email outweigh their workers’ privacy interests – even when messages contain private information. But the law sheds little light on the subject of employer monitoring of workers’ webmail, which by definition are private communications.

This paper first 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, the paper sets forth the reasons why employers monitor email. It becomes clear that the dangers of email are real and substantial. The paper then explores the technical and social measures employers use to mitigate risk of email misuse. Next, I analyze the law to the extent that it touches this issue. I find that the law clearly sanctions monitoring of work email, but that it is less clear with respect to webmail.

I also conclude that in light of legitimate business exigencies, privacy law as evolved in other contexts, and societal norms vis-à-vis email communications both 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 it pertains to wiretapping supports this notion. In addition, it conforms to the underlying policies of privacy law as embodied by the Constitution, the common law, and case law.

---

3 See Wickedpedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Webmail, (“Webmail is a Web application that allow users to access their e-mail through a Web browser, as an alternative to using an e-mail client such as Microsoft Outlook…”).
Finally, I suggest 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 Lotus Notes. Employees typically use email while at work on their employers’ premises. However, those who work remotely, such as from home, hotels, etc., can access work email through employer-provided virtual private networks.4 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 drives accountability because workers’ ideas, decisions, and actions are memorialized and easily

---

retrievable. And 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 workaday. Many businesses utilize a private, secure internal network (intranet) to enable workers to access non-public information or use internal applications.\footnote{See id. at http://en.wikipedia.org/wiki/Intranet.} But employees must often access external (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.\footnote{Deborah Fallows, Email at Work: Few Feel Overwhelmed and Most are Please with the Way Email Helps Them Do Their Jobs, Pew Internet & American Life Project, December 8, 2002.} 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. A recent study indicates that approximately eighty-six percent of workers who have work email and internet access operate them for personal use.\footnote{Nancy Flynn, 2004 Workplace Email and Instant Messaging Survey Summary, American Management Association and The ePolicy Institute (2004).} This includes shopping, corresponding with friends and family, browsing news, gossip, or personal interest sites, etc.\footnote{Id.} In 2000, for example, nearly fifty percent of online holiday purchases were made during business hours.\footnote{Russell J. McEwan & David Fish, Privacy in the Workplace, N.J. L. MAG., Feb. 2002, at 21.} Another recent study revealed that eighty-three percent of the companies surveyed had employees who use webmail to send/receive email outside the business.\footnote{Reconnex 2005 Insider Threat Index Year to Date Findings, available at http://weblog.infoworld.com/zeroday/archives/files/Reconnex%202005%20Insider%20Threat%20Findings.pdf} Just as they use work email to exchange thoughts through discussions on
business and personal topics, most workers use their webmail while at work for personal communications.\textsuperscript{11}

\section*{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. Thus far, this calculus generally justifies email monitoring in the eyes of the courts.\textsuperscript{12}

\subsection*{A. Reduce Risk of Legal Liability}

The primary reason employers monitor email is to protect against legal liability for sexual harassment, fostering hostile work environment, and fraud.\textsuperscript{13} Such liability can easily arise when employees exchange sexually explicit or otherwise offensive emails. Employers risk liability even when inappropriate emails are exchanged among consenting co-workers.

According to a recent study, seventy percent of workers have admitted to viewing or sending sexually explicit email at work.\textsuperscript{14} The threat this creates “…continues to take a hefty toll on U.S. employers, with costly lawsuits—and employee terminations—topping the list of

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{11}Id.
\item \textsuperscript{12}Kevin W. Chapman, \textit{I Spy Something Read! Employer Monitoring of Personal Employee Webmail Accounts}, 5 N.C. J.L. \& TECH. 121, 129 (2003).
\item \textsuperscript{13}See Erin M. Davis, \textit{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, 696 (2002); see also 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. 278, 279 (2003).
\item \textsuperscript{14}Chapman, \textit{supra} note 12 at 121, 23.
\end{itemize}
\end{footnotesize}
electronic risks. As recent court cases demonstrate, e-mail can sink businesses—legally and financially.”

B. Protect Assets

Protection of company assets ranks second among employers’ concerns. Email poses a threat to a company’s information technology (IT) infrastructure by serving as a conduit for harmful programs. 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. 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 trojans.

Email misuse can severely compromise a company’s intangible assets, such as its intellectual property and public image. 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.

16 Id.
17 See, Allan Carey, Managing Global Security Threats, BUSINESS TRENDS QUARTERLY, Q3 at 55 (“…the threat landscape is increasingly being dominated by attacks and malicious code that are used to commit cybercrime.”) (2006); See generally, Verizon Business, Inc., Power of Two: Presence and Precision, White Paper, WP11982 0906 (2006).
18 Chapman, supra.
19 See generally, e.g., Booker v. GET.net, 214 F. Supp. 2d 746 (D. Ky. 2002) (in which 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).
C. Prevent Loss of Productivity

Finally, employers monitor email to guard against loss of productivity stemming from excessive non-business related activity.\(^{20}\) 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.\(^{21}\) Employers, therefore, have clear, legitimate business purposes for monitoring employees’ email.

Email monitoring is relatively cheap, simple to implement, and easy to operate.\(^{22}\) 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 US employers monitor work email.\(^{23}\) Employers are also concerned with inappropriate use of the internet, with seventy-six percent of US employers monitoring their employees’ web surfing.\(^{24}\) Finally, thirty-six percent monitor all activity on employees’ computers through software that records keystrokes and screenshots.\(^{25}\)

\(^{20}\) Davis, Supra.
\(^{21}\) Id.
\(^{22}\) Because Email monitoring is largely automated, it costs less than $10.00 per employee, per year to operate. See Andrew Schulman, Chief Researcher, Workplace Surveillance Project Privacy Foundation (2001), available at http://www.sonic.net/~undoc/extent.htm.
\(^{24}\) Id.
\(^{25}\) Id.
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.

A. **How Employers Monitor Email: A Technical Review**

Most companies deploy software and equipment to monitor activity on their networks.\(^{26}\) It is technically feasible to monitor virtually 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.\(^{27}\)

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’ PCs, 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. These systems are transparent to the user, and the information 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 alert administrators to look further.

---

\(^{26}\) *Id.*

into one’s behavior. Software can even distinguish between appropriate pictures and sexually explicit pictures.  

2. On PCs

Employers can install software on workers’ computers that records every keystroke and/or captures random pictures of what is on workers’ screens (screenshots). Such software can be installed and operated without a user’s knowledge. 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 his boss’ 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.” Alas, 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 also record personal information about a user and the sites they have visited. This information is stored on the PC and can also 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

---

28 See generally, 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 Verizon).

29 For example, an employer can “push” (i.e., send) software from through its network to all connected PCs. This can be done ad hoc, for individual users, or throughout an organization. See, Client Push Installation Properties, available at http://www.microsoft.com/technet/prodtechnol/sms/smsv4/smsv4_help/a8e6b23d-41aa-4971-bc47-c6c6184affe8.mspx?mfr=true, (last visited, November 29, 2006).
such emails by using a network *packet sniffer*.\(^{30}\) This kind of 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.\(^{31}\) Such notifications typically appear in employee handbooks, at new-hire orientations, or through on-going corporate compliance trainings. These convey an implicit admonishment, to wit workers are urged to modify their expectations of privacy accordingly. For example, the following is a written policy as set forth in the employee handbook of a Verizon, a major 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.\(^{32}\)


\(^{31}\) Flynn, *supra*.

IV. **LEGAL ANALYSIS: EMPLOYER MONITORING OF WORKERS’ EMAIL IS LEGAL.**

There is no clear statutory prohibition of employer monitoring of email. Nor have the 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 – accessing the network using encryption software.\(^{33}\)

A. **Statutory Analysis**

1. **The Electronic Communications Privacy Act**

   The Electronic Communications Privacy Act (“ECPA”)\(^ {34}\) prohibits interception of email. It applies to “…any person who…intentionally intercepts, endeavors to intercept, or procures any other person to intercept…any…electronic communication…”\(^ {35}\) 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.\(^ {36}\) Work email reaches the employer’s server almost instantaneously after transmission, so there is no liability for interception, as proscribed by the

---

\(^{33}\) See infra, notes 35-38.


\(^{35}\) Id. § 2510(1)(a).

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. Consequently, webmail monitoring, theoretically, does not fall within the definition of “interception” under the ECPA.

If an employee complainant overcomes the interception-access dichotomy, he still faces two powerful exceptions that make the ECPA inapplicable to workplace email surveillance. First, the statute allows surveillance when the parties involved consent. 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 will be monitored. Many employers obtain express consent by requiring their workers to sign forms that specifically set forth email monitoring policies. But even without consent forms, courts have found implied consent when such policies are promulgated in employee handbooks. Since eighty-six percent of businesses that monitor email inform their employees of their policies, the consent exception usually applies.

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 that service…

---

37 Garrity, supra note 27 at 7-8 (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…”
40 Nancy Flynn, supra 2005.
41 Id. § 2511(2)(a)(i).
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.  

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. Not surprisingly, courts have overwhelmingly ruled in favor of employers in actions brought by employees under the ECPA.

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. 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.

Nevertheless, employers are rarely liable under the SCA because this statute also contains a “provider exception.” Furthermore, an employer does not violate the SCA if it has a legitimate business purposes for accessing employees’ stored emails. 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.

---

42 Tbg Ins. Servs. Corp. v. Superior Court, 96 Cal. App. 4th 443, 454 (Cal. Ct. App. 2002) (noting that even if an employee uses company-provided facilities 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.").


45 Id. § 2701(c)(1).

46 Id. § 2701(a)(2).
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. 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.

1. Employees Have No Reasonable Expectation of Privacy

The ECPA embraces the ruling in *Katz v. United States*, in which the Supreme Court established the principle that Fourth Amendment privacy protection applies to people who have a reasonable expectation of privacy.47 *Katz* determined that a person must have an expectation of privacy that “society is prepared to recognize as ‘reasonable.’”48 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.”49

In the context of employer surveillance of email, however, courts have ruled that employees have little or no reasonable expectation of privacy as to their work email.50 In *Smyth v. Pillsbury Co.*, the employer assured employees that it did not monitor email.51 Even so, an action for intrusion upon seclusion failed for lack of expectation of privacy.

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

---

48 Id. Katz at 350.
51 Id. *Smyth*. 

Marc Sherman 15 WEBMAIL AT WORK
management [emphasis added]. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.\textsuperscript{52}

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.”\textsuperscript{53} 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. The analysis is largely based on the relative values of business interests and employee privacy interests.

In \textit{McLaren v. Microsoft Corp.}, an employee claimed that Microsoft invaded his privacy by accessing email stored in his personal folders on his computer at work.\textsuperscript{54} Citing \textit{Smyth v. Pillsbury}, the court held that “…a reasonable person would not consider Microsoft's interception of these communications to be a highly offensive invasion.”\textsuperscript{55} 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 claimed privacy interest in those communications.”\textsuperscript{56}

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

\textsuperscript{52} \textit{Id.} at 101.
\textsuperscript{53} \textit{Restat} 2d of Torts, § 652B.
\textsuperscript{55} \textit{Id.}
\textsuperscript{56} \textit{Id.}, \textit{See also}, Garrity supra note 27, at 6-7 (“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.”).
monitoring of webmail – which belongs to the user and merely utilizes the employer’s internet access – is less clear. Webmail passes through a technical infrastructure provided, paid for, maintained, and under the control of the employer, so employers’ rationale for webmail monitoring is that all information that passes through their facilities is company property and is subject to their full control. 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., the defendant employed a crude, unsophisticated means to access plaintiff’s Hotmail account: defendant sat at plaintiff’s computer and simply guessed his password. Far from the impersonal, transparent monitoring that employers typically utilize, defendant’s act actually involved physical access to plaintiff’s real space. The court denied defendant’s motion for summary judgment despite controlling authority to the contrary, as set forth in Hillman v. Columbia County. In Hillman, the court gave undue attention to the meaning of “place,” as found in the Wisconsin statute at issue. The court was unable to reconcile the presence of the word “place” with the language in the Restatement (Second) of Torts. The court reasoned, without examining the statute’s legislative history, that the legislature was purposeful in drafting language different from the

---

57 See supra, Verizon Employee Handbook.
59 Hillman v. Columbia County, 164 Wis. 2d 376, 474 N.W.2d 913 (Ct. App. 1991).
60 Wis. Stat. § 895.50(2)(a).
61 Id.
62 See supra, note 49.
Restatement. In furtherance of its plain-meaning analysis, the Hillman court then cited a dictionary to support its conclusion that a “place is geographical.”

The Fischer court, however, understood that the word “place” in the statute “…does not limit the intrusion to a person’s immediate physical environment…” Moreover, the court stated that the issue should be interpreted in accordance with the Restatement. 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 [emphasis added] that a reasonable person would consider private…” The presence of the word “place” in the statute is merely semantic and not substantive, as summarily determined in Hillman. Casting doubt on the Hillman court’s reasoning, the Fischer court denied defendant’s motion for summary judgment, keeping alive the notion of intrusion upon seclusion in cases involving webmail in the workplace.

Another important case that deals with employer monitoring of webmail is Booker v. GET.net LLC. 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. Falsely portraying themselves as Booker, a putative customer service representative, they used the account to send a “rude” and embarrassing email to a Verizon

---

63 See supra, note 59 at 392.
64 Id.
65 Fischer, supra at 39.
66 Id. The court cited the statute itself, where it states “…the right of privacy recognized in this section shall be interpreted in accordance with the developing common law of privacy…”
67 Id. at 39-40.
68 See Lisa Infield-Harm, 2004 Wis. L. Rev. 1781, 1782, (noting that “[i]n 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].”).
69 Booker, supra note 13 at 747.
customer. Booker’s management initially blamed her for the email. Verizon interrogated her and soon understood that she was not the author. After the investigation, Booker sued the company for emotional and psychological injuries on a theory of vicarious liability. Her claim failed because she was unable to show that the tortfeasors’ committed their act within the scope of their employment. 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 spatial and temporal limits of the employment; (3) whether the action was in furtherance of the employer's business; and (4) whether the conduct, though unauthorized, was expectable in view of the employee's duties.”

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

*Booker* draws a dim line between webmail and work email. Although involved webmail use on the employer’s premises and during business hours, it was sufficiently distinct from work email such that its effects were not imputed to the employer for purposes of vicarious liability. This delineation suggests the presence of boundaries between webmail and work email and,

---

70 *Id.* at 747-48, (excerpts from the offending email read as follows: “…You [customer]…are pathetic…If you are having this much trouble getting [service], then go [to] another company…why don't you put on your pampers…OR cancel the service altogether!...You sir are a grumpy, horrible man who needs to grow up and realize that you are on earth…if you want to waste precious time spreading libel around about Verizon, which by the way is illegal, then that is your business. Please stop sending me these despicable emails at once...Sincerely, [plaintiff]”).

71 *Id.*

72 *Id.* at 746-49.

73 *Id.* at 746-50.

74 *Id.*
furthermore, that the boundaries do influence the rights of employers and employees. *Booker* faintly supports the notion that employers do not have the same carte blanch rights to monitor webmail as they do work email.

V. **NORMATIVE ANALYSIS: WEBMAIL AT WORK SHOULD BE PROTECTED.**

The common law of torts gives individuals the right to sue when one intrudes upon their seclusion or solitude in a manner that is highly offensive to the reasonable person. Similarly, one must have an objectively reasonable expectation of privacy. 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.

The 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 nations, American privacy law is excessively particular.\(^75\) This is thought to be a weakness, but this structure draws an interesting picture of American values as they pertain to privacy interests.\(^76\) 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.\(^77\) The murder of actress Rebecca Schaeffer, whose killer found her


\(^{76}\) See id. at p. 15, (noting that the European Union ranks US data-protection policies among Third World countries, to wit such policies are “inadequate.”).

\(^{77}\) 18 U.S.C. § 2710.
address through the Department of Motor Vehicles, led to the Drivers Privacy Protection Act. And the Children’s Online Privacy Protection Act protects children under the age of 13 on the internet. In addition to these federal laws, there is an abundant body of state law. 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 committed by the government or a private entity. There is widespread ignorance of general business practices that threaten privacy. But that does not translate into apathy. Americans want their privacy and they expect it – often times even when it has already been compromised. 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. Among these employees, many perceive email monitoring as a threat to their privacy.

---

81 See id. Joseph Turow, Lauren Feldman, and Kimberly Meltzer, Open to Exploitation: American Shoppers Online and Offline, The Annenberg Public Policy Center of the University of Pennsylvania, June 1, 2005.
83 See supra, note 62.
84 See Flynn supra, note 16.
exchange personal email while at work. \(^{86}\) 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 protects against employer monitoring of employee phone calls. Under the ECPA, such monitoring is only allowed if an employee consents or if monitoring is conducted in the ordinary course of business. \(^{87}\) Although these requirements are similar to those employers face for email monitoring under the ECPA, the courts have construed the statute much more strictly (i.e., in favor of privacy rights) in the context of telephone monitoring. Stricter still is the protection of postal mail. Federal law has made it a criminal offense to open another’s mail. \(^{88}\) Courts have even found intrusion upon seclusion when an employer reads an employee’s private mail. \(^{89}\) But “[t]he law has endorsed the broad monitoring of email and internet use by employers and in effect pronounced that such actions are not illegal.” \(^{90}\)

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. \(^{91}\) “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.” \(^{92}\) If so, then the day will come when the law will align with both business needs to monitor employees and societal norms,

\(^{86}\) See Flynn \textit{supra}, note 6.


\(^{88}\) See 18 U.S.C. § 1702.

\(^{89}\) Vernars v. Young, 539 F.2d 966 (3d Cir. 1976).

\(^{90}\) Gaia Bernstein, \textit{supra}.

\(^{91}\) See \textit{supra}, notes 58 and 59;

\(^{92}\) Ken Gormley, One Hundred Years of Privacy, \textit{Wis. L. Rev.} 1335 (1992).
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.”

Forty years later, the Court reversed, holding that “[t]he 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.”

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 – media used prolifically for personal as well as business correspondence. Most employers accept the reality that workers will inevitably make personal phone calls during the 8 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, et al. Similarly, the realities of the modern workaday compel workers to use webmail for non-business purposes. It follows logically 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.\textsuperscript{95} “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.”\textsuperscript{96} Employers face daunting costs when peeved workers are provoked to leave.\textsuperscript{97} Particularly in competitive job markets when businesses 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 overarching 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 that they are under surveillance, employers should explain the reasons why. If

\textsuperscript{97} See Ross Blake, Employee Retention: What Employee Turnover Really Costs Your Company, Webpronews.com, available at http://www.webpronews.com/expertarticles/expertarticles/wpn-62-20060724EmployeeRetentionWhatEmployeeTurnoverReallyCostsYourCompany.html, (published, July 24, 2006), (quoting estimates that “…It 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!”).
workers are educated about the legitimate risks as well as the protective measures, they are more likely to empathize with their employers’ policies rather 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.”

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 should implement network controls to physically bar access to as many webmail sites as possible. Sixty-five percent of companies already block access to internet sites they consider to be inappropriate. 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 Hotmail, Gmail, Yahoo, AOL, etc. 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.

**CONCLUSION**

“Everything that is really great and inspiring is created by the individual who can labor in freedom.” This bit of wisdom comes from Albert Einstein, a humble man always wary of

---

98 Flynn *supra*, note 75.
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 company leaders accountable to shareholders, multi-million dollar lawsuits are powerful 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.

---

100 Tony Phillips, Was Einstein a Space Alien? (“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.”), Science@Nasa, available at http://science.nasa.gov/headlines/y2005/23mar_spacealien.htm, (March 23, 2005).