UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 5
Issue 1 *Fall 2003*

Article 9

10-1-2003

I Spy Something Read - Employer Monitoring of Personal Employee Webmail Accounts

Kevin W. Chapman

I Spy Something Read! Employer Monitoring of Personal Employee Webmail Accounts

Kevin W. Chapman[1]

An employee arrives at work, logs onto Hotmail, types a quick message to his wife, sends a quick e-mail to friends about catching tonight's game at the bar, and forwards the latest joke that is a little risqué. This type of e-mail use is common in corporate America among employers of all sizes. However, use of personal e-mail at work is no minor distraction. Consider an average size company of 1,000 employees—if the employees spend only one hour of each day on the Internet or using e-mail, the cost to the company could be greater than $35 million dollars in lost productivity in one year.[2] Major companies such as Xerox, the New York Times, Chevron, and Microsoft have been forced either to fire employees or settle lawsuits relating to e-mail use at work.[3] Recently, employees have shifted to using personal, web-based e-mails at work.[4] Recognizing these problems, employers are now using surveillance software, known as "spyware," that can "capture every keystroke a user types at a computer, or take screen shots at regular interval[s] of everything a computer user does. [This] include[s] logging Web-based e-mail activity."[5]

E-mail use is commonplace in work environments. Some use is for legitimate business purposes, but much is for personal purposes: corresponding with family and friends, forwarding the latest jokes, or planning social events. E-mail is a valuable resource for employers. At the same time, however, it poses many

[1] J.D. Candidate, University of North Carolina School of Law, 2005.
[2] Dan Verton, *Employers OK with e-surfing*, *at* http://www.computerworld.com /managementtopics/ebusiness/story/0,10801,55344,00.html (Dec. 18, 2000) (on file with the North Carolina Journal of Law & Technology).
[3] Michelle Conlin, *Workers, Surf at Your Own Risk*, BUS. WK., June 12, 2000, at 105.
[4] Bob Sullivan, *Who's spying on my Hotmail?*, *at* http://www.msnbc.com /news/800409.asp (Aug. 28, 2002) (on file with the North Carolina Journal of Law & Technology).
[5] *Id.*

risks and problems.[6] Many companies are choosing to monitor their employees' use of electronic resources such as e-mail, the Internet, and instant messaging.[7] Companies also are implementing policies outlining to employees what kinds of information can and cannot be accessed from work.[8] These "rules, policies and monitoring tools are designed to protect . . . companies [human and financial] assets, future and reputation."[9] However, the existence of employer monitoring has resulted in some friction between employers and employees, as evidenced by recent litigation.

This Recent Development focuses on a specific type of surveillance: private employers' monitoring of their employees' personal webmail accounts, such as Yahoo or Hotmail. First, this Recent Development reviews two recent district court decisions that involve employee use of web-based e-mail accounts at work. The Recent Development then argues that given the unsettled state of the law of employer e-mail surveillance of webmail, the courts should expand the laws allowing employer monitoring to explicitly include personal employee webmail accounts accessed by employees on company computer networks or Internet connections. Finally, this Recent Development suggests ways

---

[6] William C. Gleisner, III, Michael J. Kuborn & Michael McCrystal, *Coping With the Legal Perils of Employee Email*, 72 WIS. LAW. 10, 11 (1999) (suggesting that several potential problems e-mail can create include: company liability for harassing e-mails sent by an employee, distribution of pornography via e-mail, libelous e-mails, release of confidential information and loss of trade secrets from e-mail use).

[7] A recent study "found that 14 million employees in the United States . . . have their Internet or e-mail use at work under continuous surveillance." Worldwide, that number is estimated to be around 27 million. Monte Enbysk, *Should you monitor your employees' Web use?*, *at* Microsoft bCentral, http://www.bcentral.com/articles/enbysk/156.asp (last visited Oct. 28, 2003) (on file with the North Carolina Journal of Law & Technology).

[8] AMERICAN MGMT. ASS'N, 2001 AMA STUDY, WORKPLACE MONITORING & SURVEILLANCE: POLICIES AND PRACTICES, 2001, *at* http://www.amanet.org/research/pdfs/emsfu_short.pdf [hereinafter 2001 AMA STUDY] (last visited Oct. 26, 2003) (on file with the North Carolina Journal of Law & Technology).

[9] Helen Jung, *Watching what you write*, NEWS & OBSERVER (Raleigh, N.C.), Sept. 7, 2003, at 14E (quoting Nancy Flynn, executive director of the ePolicy Institute).

employers can ensure that e-mail monitoring policies will withstand employee challenges.

I. Reasons for Monitoring

Employers give three main reasons for electronically monitoring employee e-mail use: minimizing liability, avoiding reduction in employee productivity, and protecting company assets.[10] Employers consider legal liability the foremost reason to monitor employee e-mail. Employee use of e-mail at work can result in sexual or racial harassment, fraud, libel or securities fraud claims.[11] Furthermore, most viruses are spread through use of e-mail. An employee can unknowingly spread virus-infected e-mails to others, exposing the company to tremendous liability. The cost of downtime alone, while networks are repaired, can be a tremendous expense to employers.

Second, employers are concerned that personal Internet and e-mail use decreases employee productivity.[12] A recent American Management Association study reported that nearly half of all employers surveyed explained that a very important reason for monitoring e-mail and Internet use in the workplace is to measure employee productivity.[13] Studies show that employee use of Internet and e-mail while at work is staggering—one recent study claims that "70% of employees admit to viewing or sending adult-oriented personal e-mail while at work."[14] A more recent article quotes even more astounding statistics regarding Internet and e-mail use at the workplace: more than eighty-five percent of employees use e-mail at work for personal activities, and during the 2000 Christmas season, forty-six percent of online shopping

[10] Russell J. McEwan & David Fish, *Privacy in the Workplace*, N.J. L. MAG., Feb. 2002, at 20.

[11] 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).

[12] 2001 AMA Study, *supra* note 8.

[13] *Id.*

[14] Conlin, *supra* note 3, at 106 (quoting a study by NFO Worldwide, American Management Association, Vault.com).

was done while at work.[15] Even if these statistics are inflated it becomes obvious that time spent on personal e-mail and Internet use can quickly add up, distracting an employee's attention from work. This leads to decreased worker productivity.[16]

Finally, companies monitor e-mail usage to protect their assets.[17] Theft, unapproved sharing of trade secrets, embezzlement, and destruction or damage to computer resources via a virus are major concerns when employees use web-based e-mail programs.[18] Employers may be particularly concerned about the loss of confidential information or client lists in certain work environments. Monitoring, therefore, serves as a deterrent to employees who may share this information with outside sources.

II. Employee Causes of Action

Employees seeking legal recourse against employers for monitoring personal e-mail accounts accessed at work usually will seek one of two avenues. Federal statutes relating to the interception and storing of information may be applicable. Additionally, employees may seek legal action against their employers based on the theory of common law invasion of privacy. Both of these causes of action are important because they are applicable in situations involving the monitoring of personal, web-based e-mail.

A. Federal Statutes

The Electronic Communications Privacy Act ("ECPA"),[19] which amended the Wiretap Act,[20] "prohibits the intentional

---

[15] McEwan, *supra* note 10, at 21.

[16] Conlin, *supra* note 3 (noting that "cyber-loafing accounts for 30% to 40% of lost worker productivity, according to . . . International Data Corp.").

[17] McEwan, *supra* note 10, at 20–21.

[18] A recent virus is believed to have cost over $100 million dollars in damages due to computer hardware and software damages as well as lost business and productivity. *Id.*

[19] 18 U.S.C. § 2510 (2000).

[20] *Id.* §§ 2510–22. "[The] ECPA amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral

interception of wire, oral or electronic communications and the intentional disclosure of the contents . . . by one knowing or having reason to know that the information was obtained through an interception that violates the act."[21] To violate the ECPA, the acquisition of communication must occur *during* the transmission, not after the e-mail is received.[22] Accessing stored, opened e-mail after receipt is not considered "intercepting" under the ECPA.[23]

The Wiretap Act does have two relevant exceptions. The first exception applies when one party to the transaction consents to being monitored.[24] This is why many employers require their employees to consent to monitoring. If a company has a consent form, in writing, signed by the employee, the likelihood of that employee successfully bringing suit under the ECPA is significantly reduced. Some courts have even found implied consent where employees were notified of a company e-mail

---

and wire communications." This Act now provides a private right of action "against one who intentionally intercepts, [or] endeavors to intercept . . . any wire, oral, or electronic communication." Prior to the ECPA, the Wiretap Act only applied this protection to oral and wire communications. Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak Inc.), 329 F.3d 9, 18 (1st Cir. 2003).

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

[22] Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *8 (D. Mass. May 7, 2002); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 634 (E.D. Pa. 2001).

[23] *Fraser*, 135 F. Supp. 2d at 635 (noting that accessing an e-mail post receipt is not intercepting it and thus does not violate the ECPA and comparing this post receipt viewing to finding an already opened letter sent via the U.S. Postal Service on a co-worker's desk and reading it, which would not amount to interception); *see also Garrity*, 2002 U.S. Dist. LEXIS 8343, at *8 (Electronic Communications Privacy Act "requires that the acquisition of electronic communications occur during transmission."); Steve Jackson Games Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

[24] 18 U.S.C. § 2511(2)(c) ("It shall not be unlawful under this chapter . . . for a person acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception"); *see also Pharmatrak*, 329 F.3d at 19.

policy in an employee handbook, but still choose to use e-mail for personal use.[25]

The second exception to the ECPA is the "provider exception." Providers of e-mail service are exempt from the ECPA's prohibitions on access and its prohibitions on disclosure.[26] This exception is another justification for employers to monitor their own proprietary e-mail account system without being in violation of the ECPA.[27]

Therefore, employers will not violate the ECPA as long as they fit into one of three categories. First, employers are monitoring only post-receipt e-mails. This negates the interception requirement of the ECPA. Second, employers are providing the electronic service. This is an exception to the ECPA. Third, a consent policy is in place, another exception to the ECPA. A plain reading of the statute suggests that as few as one of these criteria would suffice, though employers should consider more.

Whereas the ECPA deals with *interception* of electronic communications, the Stored Communications Act ("SCA")[28] prevents "intentional access without authorization [of] a facility

---

[25] Corey A. Ciocchetti, *Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 26, ¶ 25 (2001); Eric P. Robinson, *Big Brother or Modern Management: E-Mail Monitoring in the Private Workplace*, 17 LAB. LAW. 311, 316–17 (2001).

[26] The ECPA provider exception is stated as follows:

> It shall not be unlawful under this chapter [18 U.S.C.S. §§ 2510–22] for a . . . provider of wire or electronic communication 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 . . . .

18 U.S.C. § 2511(2)(a)(i).

[27] Larry O. Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 359 (1995); Michele C. Kane, ELECTRONIC EMAIL AND PRIVACY, PRACTISING LAW INSTITUTE PATENTS COPYRIGHTS TRADEMARKS LITERARY PROPERTY COURSE HANDBOOK SERIES, Oct.– Nov. 1993, at 419, 438.

[28] 18 U.S.C. §§ 2701–11 (2003).

through which an electronic communication service is provided."[29] Thus, the SCA's focus is post-transmission. It generally prohibits unauthorized access to the contents of communications *while in electronic storage.*[30] Another action that would violate the SCA is the situation where someone, in this case an employer, exceeds authorization to access such stored contents.[31] In order for this to be a violation of the SCA, the employer must, in addition to overstepping its authorization, obtain, alter, or prevent the employee's authorized access to his own e-mail account.[32] Similar to the ECPA, persons or entities providing the electronic communications service are exempt under the SCA.[33] For this reason, the act usually is inapplicable in situations where an employer monitors employee use of a company, proprietary e-mail system.[34] However, the cases fail to explain how the SCA might apply to employer access to stored, personal webmail accessed from work computers via the company's Internet connection.[35]

B. Common Law Claim

Some states recognize a common law invasion of privacy claim,[36] sometimes referred to as "intrusion upon seclusion."[37]

---

[29] 18 U.S.C. § 2701(a)(1).

[30] *Id.* § 2701(a).

[31] *Id.* § 2701(a)(2).

[32] *See id.* § 2701; *see also* Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 926 (W.D. Wis. 2002) (requiring, in addition to intentionally accessing the plaintiff's Hotmail account, that the plaintiff also must show that defendants "obtained, altered or prevented his authorized access to his email account" such as by changing one's password or preventing one access to one's messages.).

[33] 18 U.S.C. § 2701(c)(1).

[34] *Id.*; Echols, *supra* note 11, at 275–76.

[35] *See Fischer*, 207 F. Supp. 2d at 924–26. The Fischer court denied the employer's motion for summary judgment. The court does not directly state whether monitoring of web-based, personal e-mails, which are accessed at work and thus would be stored in some form on the employer's machine, would be a violation of the SCA. *Id.*

[36] *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 100 (E.D. Pa. 1996); Muick v. Glenayre Elecs., 280 F.3d 741 (7th Cir. 2002); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, *8 (Tex. App. May 28,

Other states have codified this tort.[38] To prove this claim, plaintiffs must overcome two hurdles: first, the employees must show that a reasonable expectation of privacy exist and second, that the invasion of privacy was highly offensive to a reasonable person.[39] The expectation of privacy is measured not by reference to the specific employee challenging the invasion, but instead by whether the employee's expectation of privacy was *reasonable*.[40] This hurdle is a high one and many employees will fail to satisfy this first condition. Several court decisions have yet to get past this first requirement, holding that no reasonable expectation of privacy existed in situations where an employer was monitoring its employees' use of company proprietary e-mail accounts.[41]

Further, even if such an expectation does exist, the court also must find that a reasonable person would consider the employee monitoring to be a substantial and highly offensive invasion of privacy.[42] The courts must determine what would be "highly" offensive to a reasonable person. They often rely on the Restatement (Second) of Torts which states that "one who intentionally intrudes, physically or otherwise, upon the solitude or

---

1999); *see aslo*, Jarod J.White, *E-mail @ Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1070, 1096–97 (1997).

[37] *Smyth*, 914 F. Supp. at 100.

[38] *See, e.g.*, *Fischer*, 207 F. Supp. 2d at 927 (section 895.50(2)(a) of the Wisconsin Statutes defines invasion of privacy); Restuccia v. Burk Tech., Inc., No. 95-2125, 1996 Mass. Super. LEXIS 367, *9 (Super. Ct. Mass. Aug. 12, 1996) (providing that Massachusetts law gives a person a right against unreasonable interference with his privacy).

[39] Though not necessarily listing them in such an explicit manner, the court asks whether the intrusion would be highly offensive to a reasonable person and in doing so asks if the employee had a reasonable expectation of privacy. *Smyth*, 914 F. Supp. at 100–01; Ciocchetti, *supra* note 25.

[40] Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *3 (D. Mass. May 7, 2002).

[41] *See Smyth*, 914 F. Supp. at 100–01; *McLaren*, 1999 Tex. App. LEXIS 4103, at *13; *Garrity*, 2002 U.S. Dist. LEXIS 8343, at *5–6. *But see Restuccia*, 1996 Mass. Super. LEXIS 367, at *9 (holding that genuine issues of material fact existed as to "whether plaintiffs had a reasonable expectation of privacy in their email messages" and whether the reading thereof was an unreasonable interference with plaintiff's privacy).

[42] RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see, e.g.*, *Smyth*, 914 F. Supp. at 100; *Fischer*, 207 F. Supp. 2d at 927.

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."[43] In doing so, courts have noted that in instances of employer monitoring of company e-mail accounts, even if a reasonable expectation of privacy existed, a reasonable person would not find the viewing of the e-mail communications to be highly offensive.[44] Thus far, employees have not had much success in convincing the courts that e-mail monitoring meets the standard of "highly offensive to a reasonable person."

C. Other Causes of Action

While Fourth Amendment safeguards against unreasonable search and seizure exist, they require state action.[45] The Fourth Amendment does not apply to action by non-governmental actors, like private employers.[46] As this Recent Development focuses exclusively on the acts of private employers, Fourth Amendment claims are inapplicable.

---

[43] RESTATEMENT (SECOND) OF TORTS § 652B; *see, e.g.*, Dubbs v. Head Start Inc., 336 F.3d 1194, 1220 (10th Cir. 2003); Med. Lab. Mgmt. Consultants v. ABC, 306 F.3d 806, 812–13 (9th Cir. 2002); *Smyth*, 914 F. Supp. at 100–01.

[44] *See McLaren*, 1999 Tex. App. LEXIS 4103, at *13 (noting that the invasions would not have been seen as "highly offensive" and that the company's interests in preventing inappropriate comments and activity via e-mail would outweigh any property interest in the e-mails); *Smyth*, 914 F. Supp. at 100–01 (noting that the invasions would not be such because the employer is not requiring the employee to disclose personal information or invading personal effects such as a urinalysis or personal search would do; also noting the outweighing company interest in preventing unprofessional comments via e-mail compared with the employee's privacy interest).

[45] White, *supra* note 36, at 1091–92 (citing Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1332 (9th Cir. 1987)); Ciocchetti, *supra* note 25, ¶ 9 (citing S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 828 (1998)).

[46] Since most Americans are employed in the private sector, the Fourth Amendment right of privacy will be of little assistance in these e-mail monitoring situations. White, *supra* note 36, at 1092; Ciocchetti, *supra* note 25, ¶ 9; *see also* Gleisner, *supra* note 6, at 12.

III. Company, Proprietary and Web-based, Personal E-mail

There is a fundamental difference between company-controlled, company-provided e-mail accounts and personal, web-based accounts; each system has a different host or originator. In a company system, the employer controls and usually hosts the system on a company server. In a personal e-mail system, an independent provider, such as Yahoo or Hotmail, stores the e-mail on its server. Users can access their webmail accounts from any computer connected to the Internet via the host's webmail page, which allows for remote access.[47] While the judicial and statutory framework applicable for monitoring each type of e-mail is the same, it is easy to predict how the courts will treat proprietary e-mail system monitoring, given recent litigation. Courts normally have sided with employers in this type of monitoring situation. It is not as easy to predict, however, how the courts will treat webmail monitoring, which is where the current monitoring conflicts subsist and where the greatest legal risks exist for employers.

A. Company-hosted, Proprietary E-mail

Company-hosted or proprietary e-mail accounts are directed through a company server and installed on a company computer network.[48] E-mails sent from these accounts are stored on the company server even if employees compose or read messages on their individual machines.[49] Courts examining common law privacy claims related to this type of e-mail monitoring have generally sided with employers, holding that there is no reasonable expectation of privacy in a company-maintained,

---

[47] *See* Echols, *supra* note 11, at 277 (describing the process by which an employee accesses his e-mail from work and the technological details that result from that access, such as a history of websites visited); *see, e.g.*, *Learn more about Yahoo! Mail*, *at* http://edit.yahoo.com/config/form?.form=ym_signup_more_info (last accessed Nov. 7, 2003) (on file with the North Carolina Journal of Law & Technology).

[48] Echols, *supra* note 11, at 276.

[49] *Id.* at 276–77.

proprietary e-mail account.[50] These decisions are based on three primary rationales.

First, the courts have focused on the fact that e-mails are sent and received via the company, proprietary e-mail system.[51] Employees are using the company's property while on company time. Using a computer and server that belong to another tends to decrease one's expectation of privacy in the use of such devices. For example, one who used a friend's computer to send e-mails would not expect the same level of privacy as if he used his own computer to send the same e-mails. The courts have used this logic in employer monitoring situations, both when companies had written e-mail monitoring policies notifying employees of such a practice,[52] and in the absence of such policies with assurances that communications would *not* be subject to monitoring.[53] Lack of express consent is not sufficient to establish a reasonable expectation of privacy. Thus, the courts have considered the employer's interest to be of a greater weight than employee privacy concerns.[54]

Second, courts point to the fact that e-mails sent via company e-mail systems are open to forwarding by a third party which diminishes any expectation of privacy with regard to

---

[50] "Courts have generally held that employees should expect little or no privacy in e-mail sent or received through an employer's e-mail system and have thus generally rejected invasion of privacy claims." Robinson, *supra* note 25, at 326; *see, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 100–01 (E.D. Pa. 1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, *13 (Tex. App. 1999); Garrity v. John Hancock Mut. Life. Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *4–6. *But see* Restuccia v. Burk Tech., No. 95-2125, 1996 Mass. Super. LEXIS 367, at *9 (Super. Ct. Mass. 1996).

[51] *See Smyth*, 914 F. Supp. at 101.

[52] *Garrity*, 2002 U.S. Dist. LEXIS 8343, at *4–5 (noting that the company had a detailed policy about the possibility of review of e-mail messages and use, which were considered company property, and reminded employees of this policy on several occasions).

[53] *Smyth*, 914 F. Supp. at 98, 101 (asking that the company had repeatedly told employees that e-mails would remain confidential, privileged and could not be intercepted and used for purposes of termination or reprimand, yet court said no expectation of privacy existed).

[54] *Id.*

e-mails.[55] Even in cases where companies allowed employees to create folders for their e-mail or utilize password protection for their accounts, the courts still hold that this does not create a reasonable expectation of privacy.[56]

Finally, the courts turn to the second prong of the invasion of privacy test: the level of offensiveness that the intrusion would impose on a reasonable person. The courts have suggested several reasons why employee suits would not pass this hurdle. Courts take into account an employer's justifications and interests in monitoring, and have often determined that the legitimate business interests of a company achieved by monitoring far outweigh an employee's privacy concerns. Such legitimate business interests include avoiding workplace discrimination[57] or investigating theft or illegal activity.[58] The courts also stress the fact that all computers used to store, send, and receive the e-mails are owned by the employer, and are thus company property.[59] These factors have led courts to conclude that an employer monitoring employee e-mail messages on a proprietary company system, for legitimate purposes, does not rise to the level of being highly offensive to a reasonable person.[60]

---

[55] In *Garrity*, the court addressed the issue of whether a reasonable expectation of privacy existed by examining the plaintiff's statements, one of which was that "[they] assumed that the recipients of their messages might forward them to others. . . . [Plaintiff] testified that the e-mails he sent to his wife would eventually be sent to third parties." The court considered the ability to forward e-mail as evidence of a lowered expectation of privacy. *Garrity*, 2002 U.S. Dist. LEXIS 8343, at *4.

[56] *Id.* at *5 (holding that courts have flatly rejected such arguments as creating a reasonable expectation of privacy so that monitoring would become an invasion of privacy); *McLaren*, 1999 Tex. App. LEXIS 4103, at *12.

[57] *Garrity*, 2002 U.S. Dist. LEXIS 8343, at *6 (noting that employer's business interests in protecting others from harassment would "likely trump . . . privacy interests" and Title VII of the Civil Rights Act of 1964 requires companies to investigate conduct when it is discovered).

[58] *McLaren*, 1999 Tex. App. LEXIS 4103, at *13 (these reasons outweigh the claimed privacy interest in the communication); *Smyth*, 914 F. Supp. at 101.

[59] Echols, *supra* note 11, at 285–86.

[60] *Smyth*, 914 F. Supp. at 101; *McLaren*, 1999 Tex. App. LEXIS 4103, at *13.

B. Web-based Personal E-mail Accounts

As employers increase monitoring of employee company e-mail accounts, employees inevitably feel more secure using their personal web-based e-mail accounts, such as Yahoo, Hotmail, and Earthlink, for personal use while at work.[61] Unlike company e-mail accounts, web-based e-mail accounts do not automatically store all messages sent and received on the company server. They are, instead, stored on the Internet company's server that provides or hosts the account.[62] However, if employees wish to access these personal accounts at work, they must use their employers' computers and Internet connections to do so.[63] New technology now allows employers to monitor these web-based accounts.[64] This technology allows them to monitor e-mail messages, record keystrokes, and even take screenshots of what appears on an employee's computer screen.[65] However, because the case history and statutory interpretations of this type of monitoring are relatively new and undeveloped, employers face less certain legal outcomes.[66]

1. Caselaw on Monitoring Web-based Personal E-mail

Two primary cases have dealt with employee suits regarding employer monitoring or intrusion upon personal, web-

---

[61] *See* Sullivan, *supra* note 4 (explaining that office workers now commonly set up free web-based e-mail accounts through such providers to "separate their work and private affairs").

[62] Echols, *supra* note 11, at 277.

[63] *Id.*

[64] Sullivan, *supra* note 4 (The new eBlaster "spyware" "will secretly forward all e-mail coming and going through [such] Web-based accounts to a spy's e-mail, allowing anyone to 'ride along' even the supposedly private email.").

[65] Enbysk, *supra* note 7.

[66] Echols, *supra* note 11, at 290 (Employers monitoring personal webmail accounts "do not have such a strong legal position as they do when monitoring only company, proprietary e-mail accounts.").

based e-mail accounts accessed from work: *Fischer v. Mt. Olive Lutheran Church*,[67] and *Booker v. GTE.net*.[68]

i. *Fischer v. Mt. Olive Lutheran Church*

In *Fischer v. Mt. Olive Lutheran Church*, co-workers overheard Fischer, a children's pastor, discussing acts of a homosexual nature on the church phone. After sending Fischer home, the senior pastor, in response to a police recommendation, hired a technology expert to examine the church's computer.[69] Fischer had his own personal, web-based Hotmail account, which he accessed from the church's computer via the church Internet connection.[70] The Hotmail account was password protected; however, with a suggestion from the senior pastor, the expert was able to guess the password and gain entry to the account through the Hotmail internet site.[71] That day, and on at least two subsequent occasions, the expert and senior pastor viewed and printed the messages found in Fischer's personal Hotmail account.[72] Fischer had not used the church's computer to read all of these messages that existed in his account at the time the senior pastor viewed them. In defense of the church officials' actions, the church claimed the officials needed to ensure that Fischer had not made improper communications with minors whom he pastored. The elders and church members subsequently voted to remove Fischer from his position for which he sued, claiming a violation of his privacy relating to the accessing of his Hotmail account.[73]

The court examined the accessing of Fischer's e-mail account under the Electronic Communication Storage Act ("ECSA"),[74] also known as the Stored Communications Act

[67] 207 F. Supp. 2d 914 (W.D. Wis. 2002).
[68] 214 F. Supp. 2d 746 (E.D. Ky. 2002).
[69] *See Fischer*, 207 F. Supp. 2d at 920.
[70] *Id.* at 917, 920.
[71] *Id.* at 920.
[72] *Id.* at 920–21.
[73] *Id.* at 920, 927. Fisher also sued for monitoring of his phone conversation that day by his co-workers; however, for purposes of this discussion it is only necessary to focus on the e-mail monitoring issue. *Id.*
[74] *See* 18 U.S.C. § 2701 (2000).

("SCA"). Congress added this act to the Wiretap Act[75] in 1986.[76] The Wiretap Act (also referred to as the ECPA) protects e-mail messages from *interception* while being transmitted,[77] whereas the SCA "indicates that an e-mail message is protected while *stored* at 'a facility through which electronic communication service is provided.'"[78]

Prior decisions have held that an employer may access stored proprietary e-mail and not be in violation of the SCA, so long as that e-mail was stored on the employer's server.[79] This is the provider exception. In *Fischer*, however, the senior pastor and expert "accessed plaintiff's e-mail while it was stored on a remote, web-based server that is owned by Microsoft, an electronic communication service provider."[80] The court never directly addressed whether the actions in *Fischer* constitute a violation of the SCA. Instead, noting an unresolved additional requirement necessary to amount to a violation,[81] the court denied the employer's motion for summary judgment and left this to the factfinder.

To fully understand the impact and limitations of monitoring declared in *Fischer*, it is important to understand the holding of *Fraser v. Nationwide Mutual Insurance Co.*[82] *Fraser* is a critical case because it interprets the ECPA and SCA as they relate to the monitoring of e-mail accounts. In *Fraser*, a company's e-mail history was examined by the employer and incriminating evidence, gleaned from employee e-mails, was used

---

[75] *Id.* § 2511.

[76] *Fischer*, 207 F. Supp. 2d at 924.

[77] *Id.* (citing United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976)).

[78] *Id.* (citing 18 U.S.C. § 2701(a)) (emphasis added); *see also* United States v. Moriarity, 962 F. Supp. 217, 221 (D. Mass. 1997).

[79] *See* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 637 (E.D. Pa. 2001) (providing that no violation of SCA occurred where an employer accessed an employee's e-mail located on the employer's server after the recipient downloaded it to his hard drive).

[80] *Fischer*, 207 F. Supp. 2d at 925.

[81] *Id.* at 926 ("Accessing plaintiff's Hotmail account intentionally is not enough in and of itself to violate the act. Plaintiff must also show that defendants obtained, altered, or prevented his authorized access to his email account.").

[82] *Fraser*, 135 F. Supp. 2d at 623.

to terminate the employee's agent agreement with employer.[83] The *Fraser* case sets preliminary boundaries as to acceptable monitoring behavior within the statutes' realms, which, when coupled with *Fischer*, provide a partial road map for employers. Within the preliminary boundaries, employers may monitor company, proprietary e-mail. E-mail which is classified as "post-receipt" is not being intercepted and thus may be monitored. Finally, if monitoring webmail, employers should avoid preventing the employee access to his own personal account.

The *Fraser* court declared that the ECPA could not be used to hold employers liable for monitoring e-mails already in post-transmission storage because "retrieval of a message from storage after transmission is complete is not 'interception' under the Act."[84] Interception of e-mails prior to receipt, however, does appear to constitute a violation of the ECPA. This would be true in both web-based e-mail and company e-mail account monitoring.

Given the distinction the *Fraser* court makes between e-mails in transit and those that are post-transmission, it is important to differentiate between the two types in cases involving web-based e-mail monitoring such as *Fischer*. The first type of e-mail is accessed from work and stored on the employer's computer or server.[85] In all likelihood this would equate to post-transmission e-mails. The other type of e-mail, unretrieved e-mail, is that which is not accessed via the employer's Internet connection, but is housed on the Internet service provider's server and accessed remotely by the employer from a location other than work.

---

[83] *Id.* at 631.

[84] *Id.* at 635.

[85] When employees send e-mails, "[t]he central computer routing the messages stores the transmissions in unencrypted plain text files available to the service provider, whether that be a third-party common carrier or the employer itself." Gantt, *supra* note 27, at 349; *see also* Echols, *supra* note 11, at 276–77 ("Every e-mail that is sent or received on the company proprietary e-mail account is stored on the company server . . . . [T]he employer has unfettered access to the stored e-mails . . . ." Web-based personal e-mails are not stored on a company server, "[b]ut a history of websites visited by the employee is stored on the company server . . . . [T]he e-mails sent and received from the web-based account are stored on the server of the Internet company . . . ."); *Fraser*, 135 F. Supp. 2d at 633–34 (differentiating between intermediate stages, back-up protection stages, and post-transmission stages of storing).

Unfortunately, the courts have not explicitly stated whether monitoring either of these types of e-mails would be a violation of the SCA.

By failing to state what types of webmail monitoring guided its decision to dismiss the summary judgment motion, *Fischer*, unfortunately, does not provide much guidance on this topic either. The court most likely failed to make this distinction because of a disagreement between the parties over the existence of certain e-mails. The court noted that "if defendants' version of the facts is correct, [that the e-mails existed and defendant obtained access to them] they would have obtained plaintiff's e-mail in violation of the act."[86] In making this statement, however, the court does not make it clear whether they are referring to those e-mails read by plaintiff from work or those that were never accessed.[87] This is an important distinction because it would allow for accuracy in predicting what types of monitoring of webmail employers can engage in and feel confident about gaining summary judgment.

Even though *Fischer* does not explicitly identify what types of webmail monitoring will constitute violations of the ECPA and SCA, the decision to deny the employer's motion for summary judgment can, at a minimum, help set some boundaries for *webmail* monitoring. The *Fischer* court did suggest that had defendants prevented the plaintiff's access to his e-mail account by changing the password that might have constituted a violation of

[86] *Fischer*, 207 F. Supp. 2d at 926 (though not clear, it appears that the court is stating that only the e-mails accessed by defendant which had not been viewed at work and were obtained by way of the password violation would constitute a violation of the act); *see also* 18 U.S.C. § 2701(a)(2) (2000) (accessing the e-mail account would have been a violation because defendant would have "intentionally exceed[ed] an authorization to access that facility and thereby obtain[ed or] alter[ed] . . . a wire or electronic communication while it is in electronic storage in such system . . . .").

[87] The likely assumption is that the court is referring to possible e-mails never checked on the church's computer, because the employee does not appear to challenge the existence of the supposed e-mail that was checked at work on the day the events transpired.

the SCA.[88] This provides some statutory guidance in that the court applies 18 U.S.C. § 2701(a)(2) of the SCA to a webmail monitoring context. The court suggests that employers who access an employee's webmail accounts without authority and then proceed to block that employee's access to his own account will be in violation of the SCA. Employers now know to avoid webmail monitoring of this aspect.

Returning to *Fraser*, there is caselaw and statutory authority establishing that the monitoring of a company's own e-mail system will not amount to interception under the ECPA for two reasons: first, an e-mail housed on the company system is not "intercepted" by the employer;[89] and, second, it falls under the provider exception of the ECPA because the employer provides the e-mail network system.[90] This narrows the area of uncertainty in the law of employee e-mail monitoring to two types of e-mail: first, those personal, web-based e-mails accessed from work, and presumably stored in some form on the employer's computer or network, and, second, those never accessed from work and stored on the remote sever of the webmail service provider. Situations such as the one in *Fischer*, where unretrieved webmail messages, never read at work, are able to be accessed by the employer, are rare considering the difficulty that an employer would have gaining access to an employee's complete webmail account. Short of guessing the password or happening upon an open webmail account on an employee's screen, an employer would face difficulty in examining e-mails never read from the work computer. This really leaves only one area of monitoring as possible and also unaddressed by the courts. Therefore, the most relevant issue is whether an employer should be able to monitor web-based e-mails, accessed and read at work, or e-mails

---

[88] *Fischer*, 207 F. Supp. 2d at 926 (finding this would mean that defendant prevented plaintiff's authorized access to his e-mail in violation of 18 U.S.C. § 2701(a)(2)).

[89] *See Fraser*, 135 F. Supp. 2d at 634–35; *see also* Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *7–8 (D. Mass. May 7, 2002); Restuccia v. Burk Tech., 1996 Mass. Super. LEXIS 367, at *6 (Super. Ct. Mass. Apr. 12, 1996).

[90] 18 U.S.C. § 2511(2)(a)(i).

composed and sent from an employer-provided computer or Internet connection.

In dicta, the *Fischer* court declined the chance to comment on whether *Fraser* correctly held that "the act [SCA] can be violated *only* by accessing e-mail that has not yet been downloaded to the recipient's hard drive."[91] It is uncertain if the acquiescence of *Fraser*'s SCA holding means the court condones the accessing of e-mail downloaded to a company computer.[92] If *Fischer* was implicitly approving *Fraser*, then *Fraser*'s post-transmission argument could be extended to allow companies to view personal, web-based e-mail exchanges that have been downloaded, stored, and are accessible from the employer's company computers. An employer who examines an employee's hard drive, searches the history feature of Internet Explorer, or examines cookies saved by the computer may be acting legitimately under the *Fraser* holding because the monitoring would be "post-transmission."

In fact, there is strong support for the theory that the *Fischer* court was concerned not with the monitoring of stored webmail, but with the actions the defendants took to access e-mails employees did not read at work. First, perhaps the strongest support is the fact that the court never mentions access to anything on the employer's server, only access to the messages on the remote Hotmail server, hosted by Microsoft. This suggests the court has no reservations about the monitoring of the e-mail accessed on the church computer. Both company provided e-mail and web-based e-mails read at work would exist on the employer's server or local computer. Second, the court may be concerned that Fischer was able to make a conscious choice to subject the work-accessed webmails to possible monitoring. However, Fischer did not make a deliberate choice to have the other unretrieved e-mail open to being viewed by his employer. Finally, when *Fischer* referred to the possibility of a violation having occurred, it focused on two points: whether disputed messages existed, presumably not

[91] *Fischer*, 207 F. Supp. 2d at 925.

[92] *Id.* (stating that because the e-mail was stored by Microsoft and not on the employer's server, "it is unnecessary to determine whether *Fraser* held correctly that the act could be violated only by accessing email that has not yet been downloaded to the recipient's hard drive.").

accessed at work, and whether defendants prevented Fischer access to his webmail.

Therefore, the *Fischer* case does set some boundaries describing what clearly is off limits, such as changing passwords, and what is clearly within the SCA and ECPA, monitoring which is approved under *Fraser*. In summary, while the court leaves unresolved the issue of monitoring webmail, they apparently approve of monitoring web-based, personal e-mail messages accessed from work. At the same time the court appears concerned about monitoring those messages which are housed on a third-party server, accessed from locations other than work, and never retrieved on the employer's computer.

In addition to examining the monitoring of employee, personal e-mail accounts under the SCA, the *Fisher* court also analyzed the case under an invasion of privacy theory.[93] Wisconsin's invasion of privacy statute is similar to the Restatement version.[94] The defendant in *Fischer* argued that a person's e-mail account cannot be a "place" upon which someone may intrude. To guide their decision, the court looked to the Restatement's broader definition of intrusion upon seclusion, which requires intrusion upon the solitude or seclusion of someone or his private concerns which would be highly offensive to a reasonable person.[95] The court agreed that e-mail, like a medical file,[96] is not a place of a geographic nature.[97] However, under the Restatement definition, e-mail might qualify as personal belongings or a person's private concerns. The court read the Wisconsin statute broadly to coincide with the Restatement, concluding that e-mail falls under the category of a person's private belongings within the meaning of the statute.[98] Unfortunately, the court did not analyze whether this defendant's

---

[93] *Id.* at 927.

[94] *Id.* (Section 895.50(2)(a) of the Wisconsin Statutes defines one of the types of invasion of privacy as an "[i]ntrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner which is actionable for trespass.").

[95] *Id.* at 928 (citing RESTATEMENT (SECOND) OF TORTS § 652B (1976)).

[96] Hillman v. Columbia County, 474 N.W.2d 913, 919 (Wis. Ct. App. 1991).

[97] *Fischer*, 207 F. Supp. 2d at 928.

[98] *Id.*

actions amounted to an invasion of privacy under the standard of "highly offensive to a reasonable person." Instead, the court denied the motion for summary judgment, leaving this question to the fact finder.[99]

In summary, *Fischer* does not answer completely what is "highly offensive to a reasonable person," and thus, an invasion of privacy. Nor does the case outline what constitutes a violation of the SCA regarding the monitoring of web-based, personal e-mail accounts. However, this case is important because it is one of the few that provides some insight into a court's analytical process for deciding cases dealing with employer access to employee personal, web-based accounts. At the very least, the case does provide defined boundaries for what is acceptable employer monitoring.

ii. *Booker v. GTE.net LLC*

Booker v. GTE.net LLC is the second major case dealing with web-based e-mail use at work and focuses on employee utilization of personal, web-based e-mail which resulted in an attempt to hold the employer liable.[100] This case supports the premise that the respondeat superior theory alone may be enough to justify monitoring of personal, web-based e-mail accounts.[101] The situation in *Booker* may have been avoided through webmail monitoring. In *Booker*, GTE.net employees created, at work, a fake, personal, web-based e-mail account in Booker's name and sent out a rude and vengeful e-mail to one of the company's complaining customers.[102] Booker was not a GTE.net employee and had no relation to the company.[103] Booker attempted to sue the company under a theory of vicarious liability, or respondeat superior.[104] In order to recover under this theory, one must show that the tortfeasors' acts were performed in the "scope of

---

[99] *Id.*
[100] 214 F. Supp. 2d 746, 748 (E.D. Ky. 2002).
[101] Echols, *supra* note 11, at 287–88.
[102] *Booker*, 214 F. Supp. 2d at 747.
[103] *Id.*
[104] *Id.* at 748–50.

employment."[105] The court found that the employees' actions were outside the scope of employment.[106]

This case provides an important warning for employers: unmonitored use of personal, web-based e-mail accounts by employees at work could expose the employer to liability based on the theory of respondeat superior. With a monitoring system such as those currently available, the company may have been able to catch the e-mail before it was sent out, or at least correct the action in a more expedient manner. At the very least, the ability to monitor such activities would decrease a company's liability concerns. Thus, the *Booker* case lends credit to the liability rationale companies use to justify monitoring of proprietary company e-mail accounts. This holding also gives companies a supplementary reason to expand monitoring to cover personal, web-based accounts.

2. Issues Left Unaddressed by the Courts

The *Booker* and *Fischer* courts did not examine the expectation of privacy that might attach to personal, web-based e-mail accessed from work. Nonetheless, a series of cases dealing with company e-mail accounts suggest arguments that may make an impact on courts considering the issue.[107]

When an employer provides access to the Internet at work, it is presumably for work purposes. The Internet connection helps

---

[105] *Id.* at 749.

[106] Under Kentucky law, courts examine four criteria to decide when actions occur within the "scope of employment." Booker did not meet the third and fourth factors: "the action was in furtherance of the employer's business," and "the conduct though unauthorized, was expectable in view of the employee's duties." The effect of Booker's e-mail was not in furtherance of the employer's business as it actually encouraged the customer to switch phone companies. The court also noted that the conduct was unexpected since falsely creating third-party e-mail accounts and sending offensive e-mails is unusual behavior for customer service representatives. *Id.* at 749–50.

[107] *See, e.g.*, McLaren v. Microsoft Corp., 1999 Tex. App. LEXIS 4103, at *12 (Tex. App. May 28, 1999); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996); Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *3–8 (D. Mass. 2002); Muick v. Glenayre Elecs., 280 F.3d 741, 742–43 (7th Cir. 2002).

the employee do his or her job. The expectation of privacy is lower for company-provided work tools than it is for those conveniences that a company provides to employees for their personal use,[108] such as providing storage space in a personal work locker.[109] Using this logic, an employee using a computer, a company-provided work tool, will have a lowered expectation of privacy. It then follows that employees accessing personal webmails via employer-provided computers and Internet access, will also have a lower expectation of privacy. This hinges on the assumption that the Internet access and company computer are tools provided for work, and not employer-provided conveniences.

A personal locker presumably is not used for work purposes, rather it is provided purely for an employee's personal convenience.[110] However, company-hosted e-mail systems exist to help employees perform their work-related duties.[111] Internet access at work is a tool employers provide to help their employees perform their jobs in an efficient and expedient manner. Neither company e-mail systems, nor Internet access, are provided for employees' personal convenience, in the way a personal locker is. A general way to differentiate between a perk and a job performance tool would be to determine its primary purpose. Another method would be to examine whether the tool can be either directly or indirectly linked to producing revenue for the employer, or whether it is solely a cost source.[112] Many employees

---

[108] *See McLaren*, 1999 Tex. App. LEXIS 4103, at *11–12 (drawing a distinction between searching company provided lockers on which employees can place personal locks and decrypting and reading e-mails stored in password protected personal e-mail folders where employees stored personal e-mails generated by the company's e-mail system. The court was unable to conclude that "creating a personal password, manifested—and Microsoft recognized—a reasonable expectation of privacy in the contents of the email messages such that Microsoft was precluded from reviewing the messages.").

[109] K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 637 (Tex. App. 1984).

[110] *McLaren*, 1999 Tex. App. LEXIS 4103, at *11 ("[T]he locker in *Trotti* was provided to the employee for the specific purpose of storing *personal* belongings, not work items.").

[111] *Id.*

[112] Business professionals call items that have no link to revenue production or support "cost centers" or "cost sources." They do not directly or indirectly

perform significant amounts of research related to their job from their company Internet access. Thus, the employer-provided Internet access can be tied to producing revenue. A work locker is simply a convenience and no apparent relationship exists between it and the company's revenue production. Therefore, because an employer's Internet access is provided for workplace revenue production, it would be analogous to a work tool and an employee should anticipate a lower expectation of privacy in the use of such tools. Because the personal webmail account grows out of the company-provided work tool, the Internet connection, there is a decreased expectation of privacy with respect to the use of these accounts while at work.

Some commentators, however, make a distinction between the two types of e-mail accounts: personal, web-based and company, proprietary. David Sobel, general counsel of the Electronic Privacy Information Center argues that

> if a company.com account is provided to me for company business, I can assume it might be subject to monitoring . . . but if I take additional step[s] to set up a Hotmail account that I occasionally access from my desktop at work, I think that could be construed as an expression of an expectation of privacy.[113]

While this argument seems valid on the surface, in light of the method of analysis the court has applied to proprietary e-mail monitoring and the similarity between the two types of e-mail, a

---

impact revenue, but are rather expenses, in the classic accounting terminology, which decrease the company's bottom line. They exist simply as a means of convenience to the employee out of the employer's generosity. The personal locker example is a classic cost center that produces no revenue, but simply makes the employees' work life more comfortable. Another cost source would be employer-provided snacks or drinks. They simply make work life more enjoyable.

[113] Sullivan, *supra* note 4. *But see* Kim Komando, *Why you need a company policy on Internet use*, Microsoft bCentral, *at* http://www.bcentral.com/articles/komando/116.asp (last visited Oct. 28, 2003) (noting that by making your Internet policy clear, the employees know of the monitoring and have no expectation of privacy) (on file with the North Carolina Journal of Law & Technology).

strong argument can be made that the use of personal webmail accounts will *not* create an expectation of privacy. Many of the same features that have caused the courts to say that there is no expectation of privacy in company-owned e-mail accounts are also present in personal, web-based e-mail accounts.[114] Two such features include the method and manner of monitoring and employer ownership of the resources used to access the e-mail. These similarities provide a strong basis for the argument that the courts should examine expectation of privacy in webmail accounts in the same manner they do for employer-provided e-mail accounts, and reach the same conclusion—there is no reasonable expectation of privacy with regard to these types of e-mail accounts.

3. Analysis

Certain aspects of personal, web-based e-mail monitoring have been addressed by the courts, but others have not. The courts should view personal, web-based e-mail monitoring in the same manner that they view company e-mail monitoring. Given the limited caselaw on monitoring of personal, web-based e-mail, the legality of such monitoring is unclear. However, caselaw suggests that if done for legitimate business purposes, within the confines of the ECPA and SCA, and with a well-designed policy in place, companies will be able to monitor employees' webmail at work.

Based on an understanding of current caselaw,[115] employers should be able to expand their monitoring to encompass

---

[114] *See* Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 at *6 (D. Mass. May 7, 2002) (attempting to avoid harassment and discrimination in the workforce outweighs privacy interests of employees); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996); *McLaren*, 1999 Tex. App. LEXIS 4103, at *13 (preventing inappropriate and unprofessional comments, or even illegal activity are business purposes that justify monitoring).

[115] For discussion of the ECPA and the definition of "intercept," see *Garrity* 2002 U.S. Dist. LEXIS 8343, at *7–8; Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak Inc.), 329 F.3d 9, 21 (1st Cir. 2003); Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 924 (W.D. Wis. 2002); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 634–35 (E.D. Pa. 2001).

all e-mails, including those from personal web-based accounts, without violating the ECPA. Though most courts have not addressed this specific form of e-mail monitoring, the approaches companies use to avoid the ECPA's restrictions when monitoring company, proprietary accounts will also apply to personal, web-based ones. These approaches include arguing that monitoring and reviewing e-mail after receipt is not "interception," as well as obtaining consent from employees to engage in this style of e-mail supervision. Given the legal success of such strategies, companies should follow the same strategies used for monitoring company e-mail, when monitoring personal, web-based e-mail accounts. Because the ECPA covers interception of electronic communication,[116] companies need only ensure that they are not intercepting the messages, and instead are accessing them from storage. *Fraser* shows that the courts will not view this type of activity as a violation of the ECPA. Employers can further protect themselves from the ECPA's reach by obtaining consent from employees to monitor these accounts. Other than the fact that employers will not qualify under the provider exception to the ECPA, companies should use the same proactive defense strategies they have used when monitoring company, proprietary e-mail accounts to avoid ECPA violations. Following these steps, employers will avoid ECPA violations, and also fit within the statutorily-defined exceptions.

The issue of SCA violations has not been answered by the courts. Under *Fraser* logic, a company would most likely be justified in examining personal, web-based e-mail only after it has been accessed by the employee while at work. This would allow a copy of the e-mail to be stored on the company's computer which the employer may then view. However, companies should limit their monitoring to stored e-mails and avoid obtaining, altering, or preventing unauthorized access to the e-mail account to avoid violating the SCA.

The courts have given little indication of whether this new personal, web-based monitoring scheme would be a common law violation of an employee's privacy. Neither of the two prongs of

[116] 18 U.S.C. § 2511(1) (2000); *see also Fraser*, 135 F. Supp. 2d at 633.

the invasion of privacy test: whether a reasonable expectation of privacy exists nor whether the monitoring would be highly offensive to a reasonable person,[117] have been addressed directly by the courts. At this point, only inferences can be drawn from the court's reasoning in denying the common law claims in the company, proprietary e-mail monitoring cases. Once the themes and logic are identified, they can be applied to these new monitoring situations. Similarities exist between the two e-mail monitoring situations. Webmail access exists at work only through the use of company computers and the company's Internet connection. Furthermore, companies may have a policy of monitoring all Internet activity, which would include webmail accounts. Finally, the e-mail is open to future access by other parties if recipients forward the message. Company e-mail accounts share these same features, and, relying on these characteristics, the courts have held that a reasonable expectation of privacy did not exist.

In evaluating the second prong, "offensiveness to a reasonable person," inferences also must be drawn from the company e-mail monitoring cases. Just as in company e-mail monitoring, businesses still have legitimate interests to protect and presumably employees will be put on notice of possible monitoring if a policy of monitoring exists. At each point, employees make a calculated choice to have their e-mail monitored by choosing to use the employer's Internet to log on to their personal account and then again when sending and receiving personal e-mail messages at work. These have been important factors for the court to find that a reasonable person would not find the monitoring highly offensive. Because both types of monitoring share these features, the courts should hold the same for monitoring of web-based, e-mail accounts. Therefore, due to the similarity of the characteristics the court views as important, if employers follow the same procedures as they do when monitoring company, proprietary e-mail, a valid claim for invasion of privacy should not exist when monitoring personal webmail so long as it has been accessed from the company's computer and Internet access.

---

[117] *Smyth*, 914 F. Supp. at 100–01; Ciocchetti, *supra* note 25.

IV. Suggestions for Monitoring Policies

As companies react to a shift by employees from using company, proprietary e-mail accounts to personal, web-based ones, many employers will begin to monitor this type of e-mail use at work. Given the lack of case history regarding such monitoring, employers should act proactively to avoid lawsuits or develop strong defenses to combat such attacks. Several commentators have discussed strategies employers can use to implement effective monitoring policies.[118] While these may be helpful as "best practices," the current environment of personal, web-based e-mail monitoring is still relatively young and has not been extensively challenged in the courts. Given this lack of judicial history and the potential for increased employee resistance, the policies employers adopt will need to be more proactive and seek a better balance between employers' interests of security and employee sense of autonomy and privacy.[119] The following recommendations will help a company's e-mail policy establish such balance by incorporating traditional consent policy formation with creative, flexible solutions.

A. Barriers to Access: Policy Creation and Notification

1. Consent Policy

Employers need to have written e-mail monitoring policies that require employees to consent to potential monitoring of their e-mail use as a condition of employment. The policy and consent form should then be stored in employees' personnel files. In order for the consent to be effective, the monitoring policy must be explicit in its wording. This is especially important if e-mail use is

[118] *See, e.g.*, McEwan, *supra* note 10, at 23–24; Echols, *supra* note 11, at 298.

[119] Enbysk, *supra* note 7 (quoting Michael Gartenberg, research director at Jupiter Media Metrix, "[e]mployees need to understand that it is the employer's right to protect its business communications vehicles from abuse . . . ." At the same time, "[e]mployers need to understand that expectations need to be set and met, and that an appropriate balance needs to be achieved between total trust of employees and total lack of trust.").

already in existence at the time the policy is adopted.[120] The policy should note that there is no expectation of privacy in the use of such e-mail and that e-mail from the company system is company property.[121] Some employees may feel micromanaged by this policy so companies may wish to note that monitoring is a right reserved by the employer. Additionally, companies could emphasize to employees that they can use e-mail at their discretion for emergency or critical purposes, however, that use could be subject to monitoring.

To ensure that the company's policy is visible, employers may opt to have an on-screen pop-up box that is triggered any time the employee opens the web-browsing or e-mail software. Employees could remove the box only by signaling their agreement with the following statement: "I understand and comply with [COMPANY NAME]'s policy on the monitoring of and restrictions on e-mail use." This keeps employees on notice of company monitoring and requires them to make a conscious choice to accept such monitoring at each use.[122] Another suggestion employers may consider is displaying the policy in such a manner that upon initial login, the employee is presented with the policy prior to network access.[123] By logging in, employees signal their consent to monitoring by the employer.

2. Specify Web-based Personal E-mail

To make the policy more clear, companies should specifically call out and highlight the fact that the company's policy will apply to personal, web-based e-mail access, in addition to company e-mail. Making certain that employees know this e-mail is also open to monitoring will cause them to seriously consider what types of e-mail to send and receive from work. Companies should also explain that when personal e-mail is retrieved or sent via the company's server or Internet connection, there is a possibility that these e-mails may be copied onto the

[120] White, *supra* note 36, at 1103.
[121] *Id.*
[122] Komando, *supra* note 113.
[123] Echols, *supra* note 11, at 300.

computer's hard drive or company server, stored, and may be accessed by the employer at a later date.

Certain aspects of the policy should be specifically directed at the use of web-based, personal e-mail. For instance, employees should be restricted in their ability to download attachments received in their personal e-mail accounts. Employees should also be restricted from sending or receiving any business or company-related e-mail from their personal address. This ensures that clients and co-workers only communicate with the employee via the company-sanctioned proprietary account. To allow otherwise may create a decreased level of professionalism between employee, as a representative of the company, and client.

3. Selectively Block Access to Internet Sites

Depending on the size and needs of the company, some employers may choose to block the entire Internet system in certain circumstances. While this is extreme and often impossible for most companies, they should consider restricting access to certain sites they deem inappropriate for use at work, such as pornographic websites, Internet auctions, job search sites, web-based personal e-mail sites, and sports sites. Being overly restrictive sometimes affects employee morale or attitude.[124] Therefore, employers must be careful to balance the legitimate need to restrict this access with the employees' right to autonomy. Selectively blocking certain websites has two benefits. First, if webmail Internet sites, such as Yahoo.com, are blocked, then employees are never able to access their personal, web-based accounts at work and the need for monitoring of this e-mail type will not exist. Second, selective blocking allows employers to choose what Internet sites would be inappropriate, while at the same type maintaining access to sites that are used for legitimate company purposes, such as research and sales.

---

[124] Sindy J. Policy, *Employer Monitoring of Employee Internet and Email Use: An Effective Litigation Avoidance Tool*, COMPUTER & INTERNET L., Nov. 2000, at 21; Conlin, *supra* note 3 (stating that employees may question their commitment to a company that is sending the message to its workers that it does not trust them); Enbysk, *supra* note 7.

Despite these benefits, there is a possible complication that arises from selective e-mail monitoring. Besides being overbroad in some cases, employers will never be able to effectively block access to all Internet sites that provide webmail access. The proliferation of web-based e-mail accounts makes it almost impossible to block access to all of these sites. Many companies, education institutions, and organizations offer web-based e-mail accounts. Individually blocking access to each and every one of the possible web-based account sites appears impossible. However, in the right situation, for some companies, this will be the best policy and may be the most cost effective method of decreasing the greatest percentage of web-based e-mail access.

B. Alternative Employee Access

Employees may wish to utilize their own wireless laptop computers, Internet-enabled cell phones, and other non-company Internet connections to send and receive personal e-mail during work.[125] This allows employees to keep their personal messages private. The use of non-company technology still presents the employer with the problem of decreased workplace productivity, so employers may wish to suggest these options only in emergency situations. Additionally, employers may instruct employees using these technologies to conduct personal business during "time off," such as lunchtime or during breaks. This allows the employee to maintain connection during the day via e-mail, while avoiding the employers' concerns of liability and decreased productivity. This is a win-win situation for both parties.

C. Remedial Solutions

1. Penalties for Violation

Detailing the penalties for violations of the policy may help employees take the policy more seriously.[126] If employees know what the consequences are for breaking company rules, they may

[125] Echols, *supra* note 11, at 299.
[126] White, *supra* note 36, at 1103.

be more likely to comply. Not only defining the violations, but also avoiding acquiescence of violations is important. If employees view the policy as dormant, they may ignore it. Finally, companies should closely document all violations, responses, and follow-ups and place that information in the employees' personnel files. This will prevent an employee pleading ignorance to the presence of a monitoring policy to which they consented.

2. Requiring Employee Indemnification for Damage

In certain high-risk situations, such as when the nature of the employment involves sensitive company material, companies may need to take drastic action to ensure personal e-mail use does not affect them adversely. While this approach should be limited in application, some situations may dictate that employers require employees to indemnify companies in the event of any loss that arises from their use of company resources for personal e-mail. As noted, the psychological impact of this type of policy could be damaging to employee relations, so it should be reserved for situations where e-mail has high potential for disastrous effects on the company.

D. Employee Response

When suggesting how employees should act in this new era of monitoring, perhaps one professional summed it up best, "A word to the wise: Treat your e-mail system at work as you should your business phone. Strictly limit your communications with family and friends. And do not send a message if you would be uncomfortable having a co-worker or your employer read it."[127] Furthermore, "[n]ever send an e-mail . . . at work that you wouldn't be afraid to read the next day on the front page of a

[127] Barbara Kate Repa, *Computers and Email on the Job, at* http://www.hrlawinfo.com/lawguide/Privacy/computers_and_emai.asp (last visited Oct. 24, 2003) (on file with the North Carolina Journal of Law & Technology).

newspaper. . . ."[128] The best advice is to use common sense. Avoid using web-based e-mail accounts while at work and only make exceptions for employer-approved emergencies.

V. Conclusion

Now that employees are beginning to shift to using personal, web-based accounts while at work, employers are beginning to expand their monitoring practices. Relying on the limited case history that exists, coupled with the better-defined analysis of proprietary e-mail accounts, companies have support for monitoring and should be able to withstand employee lawsuits challenging such practices.

By avoiding the interception of e-mails in transmission, employers avoid vulnerability from the ECSA. Choosing a program that only monitors e-mails that are physically viewed by the employee while at work on the company computer will likely avoid the SCA's restrictions on accessing stored communications. Following the suggestions of this article in drafting a policy and consent form will allow a company to have a safety net against such statutory liability. It appears that given the similarity in the methods of monitoring, and the reasoning behind monitoring, in both proprietary and personal e-mail accounts, employers can defeat invasion of privacy claims. Close examination of the rationale and dicta of the court can flesh out hints about the direction the court may take for invasion of privacy cases that are sure to come. Since both types of monitoring share similar characteristics and logic, it stands that if employers go about the monitoring in the manner described in this article, employers will stand a good chance of withstanding an invasion of privacy claim.

As technology becomes more and more sophisticated, employers expect greater demands from their employees; employees feel pressures to better balance their work and life responsibilities; and societal pressures cause companies to seek safety and increased productivity. As such, it is inevitable that situations such as the ones addressed in this article will continue to

[128] Enbysk, *supra* note 7.

proliferate. For these reasons it is imperative that employers, employees, and all other stakeholders search for the common ground and formulate proactive solutions.