Think Before You Type: A Look at Email Privacy in the Work Place

Meir S. Hornug*
NOTE

THINK BEFORE YOU TYPE:
A LOOK AT EMAIL PRIVACY IN THE WORKPLACE

Meir S. Hornung*

INTRODUCTION

Email has rapidly become the predominant method of communication for companies around the nation and around the globe, and most experts agree that it has changed the workplace for the better.1 With the ability to widely transmit large amounts of data instantaneously, email has emerged as an essential tool for increasing productivity and efficiency in the workplace.2 One benefit email has over telephone or written communications is that all email messages are logged and recorded for future reference. However, the basic attributes of email that have vastly enhanced corporate communication have also led to a multitude of unexpected difficulties for employers. Among the problems that the escalating use of email has caused are "increased [employer] vulnerability to corporate espionage and liability for fostering a hostile work environment."3

Since email and other electronic communications are highly valuable assets to companies, employers have chosen to monitor their use rather than succumb to the difficulties and remove the technology

* J.D. candidate, May 2006, Fordham University School of Law.
3. Todd M. Wesche, Reading Your Every Keystroke: Protecting Employee Email Privacy, 1 J. HIGH TECH. L. 101 (2002). For a more detailed analysis, see infra notes 27-41 and accompanying text.
altogether. Employers believe that monitoring is necessary both to discourage illicit activity and to limit liability. The problem that monitoring presents for employers is that it “is detrimental to employee privacy and creates unnecessary stress that has a direct negative impact on emotional and physical health of the employees,” which can have a detrimental effect on work product.

The advent of email monitoring in the workplace has spawned a debate over the propriety of such practices, pitting employers’ interest in preventing misuse of their computer resources against employees’ expectation of privacy in their electronic communications. The argument over computer surveillance has been further fueled by the covert nature of most email monitoring programs. Employees claim that without some restriction on an employer’s ability to monitor email, there will be no privacy protection left in the workplace. However, employers support their claim that monitoring is necessary by pointing to the vast amount of litigation that has resulted from the unmonitored use of employee email. The debate rages on as to whether it is moral, ethical, and, most importantly for purposes of this paper, whether it is legal for employers to surreptitiously monitor the email of their employees.

This paper will attempt to analyze the laws pertaining to workplace privacy and apply these laws to the context of email monitoring by employers. Part I will be a discussion of the background of the right to privacy as it relates to the workplace. Part II will discuss the background of employer monitoring, its history, and the modern monitoring practices. Part II will also discuss the reasons employers monitor their employees’ email communications and the arguments the employees have against such monitoring. Part III will explain the common law invasion of privacy requirements, the federal statutory requirements, and the different types of email systems that currently exist. Part IV will use the courts’ analyses of email cases in order to derive general rules for determining when employers should be liable for privacy violations. Part V will briefly outline various state approaches to the email privacy question and address a variety of proposed legislation on the subject.

---

4. Id.
5. See infra notes 17-18 and accompanying text.
I. Right To Privacy In The Workplace

Employees’ distaste for monitoring is grounded in the historic right to privacy that exists in our nation. The United States Constitution may hint at this right to privacy, but it was given shape in an article written in 1890 by Samuel D. Warren and Justice Louis D. Brandeis. These esteemed authors proclaimed that “[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right ‘to be let alone.’” Warren and Brandeis knew that society and the workplace were constantly advancing and perpetually improving the way we live and work. They concluded that in order to keep up with the steady but sure changes that have occurred and will occur in the future, the American legal system had to evolve to protect this new and improved way of life along with the individual’s privacy rights. At the time that they wrote their article, only a small minority of courts had embraced the right to privacy thesis that they spoke of. However, throughout the twentieth century, the right to privacy became firmly entrenched within the American legal system.

In today’s increasingly technological world, the potential danger to individual privacy interests exists at a level never before seen. In this fast paced environment, the transmission of large pieces of information has become as quick and simple as the click of a mouse or the touch of a button. These technological advancements lead to conflicts between the interests of employers and employees. The employers have an established right to run their organization in a method that will best protect their company, while the employees have a right to privacy in

7. See infra notes 8-11 and accompanying text.
11. With the impending retirement of Justice O’Connor, the minority in Casey may have enough Justices to develop a majority, and the Supreme Court may be in position to overturn Casey, the case which granted a generally accepted right to privacy. As Chief Justice Rehnquist said in Casey, past Supreme Court decisions make clear that the Court does not “endorse any all-encompassing ‘right of privacy.’” Planned Parenthood of S.E. Pa. v. Casey, 505 U.S. 833, 951 (1992) (Rehnquist, C.J., concurring in judgment, and reversing in part, joined by White, Scalia and Thomas, JJ.).
their personal lives.\textsuperscript{12}

While the overwhelming employer response to the employee email problem has been to monitor email,\textsuperscript{13} employees have been quick to respond. Employees are challenging monitoring techniques under common law, statutes, and constitutional legal theories in attempts to maintain their privacy. Thus, while some employees may sue their employer over an offensive email they receive at work, others seek to ensure their right to send and receive such an email. Employers are caught in the middle between the rights of their employees and the responsibilities the employers have to protect themselves.\textsuperscript{14}

The emergence and widespread use of computers and email in the workplace has created many challenges for employers, their attorneys, and the courts. Specifically, courts are forced to apply traditional rules of law to modern technological advancements. Since many of the traditional rules that governed areas of privacy law focused on slow moving or stationary matters, courts are unclear how to apply these rules to email, which has resulted in ambiguity between the rights of employers and their employees.\textsuperscript{15}

Today, the notion that the scope of an employee’s right to privacy, regardless of the source of the right, is limited by the employee’s reasonable expectation of privacy is accepted as a threshold principle in evaluating workplace privacy issues.\textsuperscript{16} Assessing whether an employee’s expectation of privacy is reasonable in order to determine whether the privacy right exists has its genesis in the Fourth Amendment of the United States Constitution, which provides that any “unreasonable search and seizure”\textsuperscript{17} is unconstitutional. In analyzing the reasonableness of the search, courts often balance the need to search or intrude against the resulting invasion of privacy.\textsuperscript{18} Limitations on the

\begin{itemize}
  \item \textsuperscript{12} Baum, \textit{supra} note 9, at 1012.
  \item \textsuperscript{13} More then 85% of employers have some form of monitoring practice in place. American Management Association, \textit{supra} note 1.
  \item \textsuperscript{15} Gregory I. Rasin \& Joseph P. Moan, \textit{Fitting a Square Peg into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace}, 66 Mo. L. Rev. 793 (2001).
  \item \textsuperscript{16} See O’Connor v. Ortega, 480 U.S. 709 (1987).
  \item \textsuperscript{17} U.S. Const. amend. IV.
  \item \textsuperscript{18} This will be an underlying theme throughout this paper.
\end{itemize}
government's ability to intrude on the constitutional right to privacy have been specifically recognized where "the most basic decisions about family and parenthood" are concerned. As the Supreme Court said in *Casey*, "[i]t is settled now . . . that the Constitution places limits on a State's right to interfere with a person's most basic decisions about family and parenthood." Despite this precedent, establishing clear limitations on an employer's invasion of an individual's right to privacy in the workplace has proven to be particularly troublesome for the courts. Even where such limitations have been articulated, courts often have been unclear as to when employers' monitoring of employee email is a violation of the employees' right to privacy.

One of the reasons for the conflicting interpretations of an employee's right to privacy can be attributed to the way in which courts approach the question. When the first email privacy questions arose, courts approached the issue by comparing email privacy rights to preexisting privacy rights. The courts were uncertain whether email should be analogous to traditional mail, or if the privacy rights should parallel that of workplace lockers and desks. There was no clear cut determination of how the email issue should be approached, and consequently courts had a problem reconciling email with older forms of workplace invasions. In the last five years, courts have moved away from the traditional workplace analyses and have come to independently analyze email privacy questions. Although the courts seem to have

---


20. Casey, 505 U.S. at 849.


24. Id.

reached some uniformity in how they approach email privacy issues, the results are as disparate as they were before.  

II. EMPLOYER MONITORING OF EMPLOYEES

Employer monitoring of their employees at work is a management pastime that has been around since the birth of our nation. In the past, when the workplace was simple and everyone used a pen and paper, it was easy to hide the tracks of what you had done, but being mischievous took time. With the advent of computer use, employees could work a little faster, but their questionable actions may have been displayed on a screen for a long time and anyone walking by could look over their shoulder and watch them. In current times, with the ease of use of computers and the speed of the Internet and email, employees can carry out their rogue behavior quickly and without being noticed by any passers by. Similarly, harassing emails can be sent instantaneously, and valuable data “can be taken quickly by electronic duplication.”

This long history of employee monitoring has adapted to new technologies and employers have used these new technologies to their advantage. Monitoring software has extended to inventory and cash register systems that are programmed to detect possible theft or fraud. Global positioning systems are used to keep track of the whereabouts of employees while they are driving company vehicles. Systems have even been installed for food service and health care workers that record whether or not an employee, who enters a restroom, has stood for a specified period of time before the sink with the water running and whether or not the soap dispenser was used. The extent of the usage of such monitoring devices is not known, and has not been advertised by companies who use them. Email monitoring, however, is well known to be widely used.

26. Compare Fischer, 207 F. Supp. 2d 914 (denying employer’s motion to dismiss the employee’s privacy claim), with Fraser, 135 F. Supp. 2d 623 (granting employer’s motion to dismiss the employee’s privacy claim).


There have been several reasons given by employers to justify the monitoring of their employees' email. The basic reason is that the employers are concerned with work productivity. 29 Employers believe employees are wasting too much time reading and answering their own personal email, and consequently not doing their jobs. The primary reason for having email in the workplace is to enhance employee productivity by allowing individuals to communicate more efficiently with others. However, the copious utilization of email by employees for their own personal exploits detracts from the goals of integrating email into the corporate environment. The misuse of email reduces worker productivity and eventually diminishes company profits.

Employers also argue that their proprietary email systems become overcrowded and bogged down as a result of employee personal use, and thus that monitoring employee email is legitimate. 30 Emails that are sent to just one corporate email account can be, and often are, forwarded to dozens of other accounts on the company's email system. At first glance, the problem of filling up the company email servers does not seem to be a potentially fatal one because basic, everyday text emails do not take up much space and thus will not overcrowd a server. The problem is magnified, however, when these mass forwarded emails contain pictures, audio, or video file attachments. These emails can take up large amounts of space on the company email system, and if these emails are forwarded to many employees within the organization, there can be hundreds of copies sitting on the server, with no benefit to the corporation. The result can lead to a slowdown of the email system, and to company employees not receiving work related email in a timely fashion. At worst, if the company's email server is filled to capacity and unable to handle any new data, emails will simply be returned to their sender.

A third reason employers suggest monitoring is that it is necessary to protect company security and confidential information, which is stored inside of their company servers. 31 Employers are very concerned about the surreptitious transmission of trade secrets or other confidential information. Organizations hold a wealth of their own proprietary

29. See American Management Association, supra note 1.
30. Finkin, supra note 28, at 474.
information, as well as that of third parties including customers and suppliers, in electronic format. The ease of attaching large files to emails, and the speed with which such information can land into a competitor’s hands, have many companies fearful of the possible loss of business.

Finally, the reason that has become most costly is the concern over potential employer liability for sexual harassment arising from the transmission or display of sexually suggestive or demeaning emails through the company email system. The National Institute of Business Management (the “Institute”) has reported that if companies do not monitor the email use of their employees, they are putting their businesses at risk of being sued for employment discrimination and sexual harassment. The considerable use of email, in comparison to all other forms of communication, and the speed of the communication can quickly lead to liability for harassment and discrimination. Employers can also be liable for simply having tolerated a hostile work environment. Under the doctrine of respondeat superior, an employer can be held liable if a plaintiff can show that the actions of the employee were committed within the scope of employment or in furtherance of the employer’s interest. Courts have concluded that any employee conduct that is closely connected to a work activity is considered within the scope of their employment, even if such action is forbidden by the employer. As a result of this expansive view of employer liability, the Institute advises employers that they can and should “monitor email messages regularly for evidence of discriminatory material.”

When employers do not monitor their employees’ email, the results can be devastating. The New Jersey Supreme Court encountered this situation in *Blakey v. Continental Airlines Inc.*, which held that derogatory and potentially offensive emails posted on an employer's email system could lead to liability for sexual harassment.

---

provided system could support a hostile work environment claim under the state's anti-discrimination laws.\textsuperscript{39} The court reasoned that the email communications system is an extension of the workplace.\textsuperscript{40} Consequently, the employer's duty to prevent harassment from taking place in the workplace includes a duty to prevent harassment from taking place within the employer's email system.\textsuperscript{41}

Email, as well as all forms of Internet communication, has led to the overburdening of companies with harassment, discrimination and libel litigation.\textsuperscript{42} Exchanges on the Internet through chat rooms, email, and using instant messaging programs produce communications that are often more frank, sexually explicit, and hostile than communications in other forms. Some people mistakenly believe that they can write anything in an email without liability or responsibility. Clearly, this is not true. Copyright infringement, defamation, and harassment are examples of potential liability that both employees and companies must guard against.\textsuperscript{43}

Clearly, employers have many reasons to monitor their employees' email, but it is just as clear that employees do not want to be monitored. The obviousness of this statement is echoed by the foremost reason put forward by employees to prevent email monitoring: people generally prefer privacy over surveillance. But this argument alone may not be enough to prevent the monitoring because the Constitutional right to privacy that has arisen over the last fifty years is a limited one at best, and has been held not to affect the workplace environment.\textsuperscript{44}

There are numerous other reasons presented by employees to combat employers' desire to monitor their email. If an employee does not have privacy in the workplace, they may come to feel that their employer does not trust them. This perceived lack of trust may lower employee morale, and erode the mutual respect between an employee and employer that needs to exist in order for a successful working relationship to continue. Without this feeling of trust, employees will

\textsuperscript{39} Id. at 543.
\textsuperscript{40} Id.
\textsuperscript{41} Michael & Lidman, supra note 14.
\textsuperscript{42} Finkin, supra note 28, at 474-77.
\textsuperscript{43} See, e.g., Finkin, supra note 28, at 474-77; see also Company Computer Communications Policy, Law of the Internet § 2.11, at 1-2 (Matthew Bender 2005).
\textsuperscript{44} O'Connor v. Ortega, 480 U.S. 709 (1987). Some Supreme Court justices do not believe in any general right of privacy. See supra note 11.
not work at the same pace and with the same desire to further the company's interests. Another reason the employees give is that monitoring can result in extreme harm to the health of the monitored employees.\textsuperscript{45} Stress, depression, and anxiety often result from employer monitoring of email in the workplace.\textsuperscript{46} Employee stress may cost employers more than seventy five billion dollars annually in the form of absenteeism, turnover, poor management, higher health costs, and the avoidance of email altogether.\textsuperscript{47} Employers claim that monitoring of email is geared towards saving the company money, but in the long run it may cost the company billions of dollars in employee productivity.

Employees have proposed another theory supporting why they should be entitled to privacy in the workplace. Employers provide employees with certain technologically advanced tools such as a telephone, voicemail, email, and Internet access, all of which allow employees to accomplish more work in less time. Employees contend that the increased productivity demands of the workplace, and increased demand on the amount of time that employees spend at work, require employees to mingle their personal and professional lives.\textsuperscript{48} This is especially so when it comes to such items as email usage. Employees, therefore, believe the law in this area should recognize "such a real workplace dynamic."\textsuperscript{49} Employees need to take care of personal business in the office, and if the employee can most quickly resolve personal matters by using workplace resources, it is in the employer's best interest to allow the employee to do so. The only way for the employee to feel comfortable conducting their personal business at work is by ensuring that private business will remain private. In such an environment, where employees' handling of private matters results in a benefit to the employer in terms of higher morale, increased productivity, and more time spent at work, employees arguably should not be forced to sacrifice their privacy rights.\textsuperscript{50}

\textsuperscript{46} Id.
\textsuperscript{47} Id.
\textsuperscript{48} Fazekas, \textit{supra} note 36.
\textsuperscript{49} Id.
\textsuperscript{50} Id.
An employer will favor monitoring whenever it faces potential liability because of the actions of its employees. Inversely, employers favor employee privacy when the employer will not be held liable for the actions of its employees, because the employers understand the drawbacks of monitoring their employees. But when liability is uncertain, as is most often the case, an employer will seek to protect its own interests. Since liability is typically decided based on the facts of an individual case, and is only determined after an employee has already acted, it is impossible for an employer to grant employees the complete privacy the employees would like while still avoiding its own liability.

One factor that is used in weighing the propriety of email monitoring is the invasiveness of the technology the employer uses to monitor. Employer monitoring of company owned proprietary email accounts does not require much extra work by the company management. All email that is sent or received through the system is stored in the server and can be viewed later. Both the intended recipient and anyone with proper administrative access to the server can read all email messages stored on the server. No additional software or hardware needs to be installed on the company network or on the individual computers in order for the monitoring to take place. The reason for this is that the storage of email is a necessary component of a company email system. The storage of email is primarily intended for use by the end user so that they can store their email for later viewing or reference. One consequence of the storage is that anyone with access to the servers can view everyone's email. The only additional requirement to convert a basic email system into an employee monitoring system is to have someone spend the time reviewing the employees' email.

In order for an employer to monitor an employee's personal, web-based email, such as Yahoo, Hotmail, or Gmail, the employers have to exert a little more effort. New technology allows employers to monitor web-based email messages and chat conversations, record keystrokes, and take screenshots of what appears on an employee's screen. To use this new technology, employers must install additional software or

51. Echols, supra note 45, at 277.
52. Id.
54. One example of this is the Family Keylogger program, http://www.spyarsenal.com (last visited Nov. 21, 2005).
hardware directly onto an employee's computer.\textsuperscript{55} These supplementary programs record the designated information, and, in most instances, periodically email the stored files to a supervisor.\textsuperscript{56} However, with some monitoring technologies, the employer must retrieve the information from the target computer itself.\textsuperscript{57}

These types of automated employee monitoring software systems have become very sophisticated. These systems can record, filter, and sort every word of every email that employees type.\textsuperscript{58} Even software that has a core purpose other than to monitor email, such as anti-virus and spam blocking software, can be used creatively to monitor. Applications such as pcAnywhere allow remote computer system administrators to view the computer screens of users in real-time, and can be used to monitor unsuspecting employees’ computer activities. Monitoring comes in many forms and can be done without an employee's knowledge or detection. Often, such systems are installed without any notification to employees that their email is being monitored.\textsuperscript{59}

The makers of the monitoring software are aware of the possible abuses of their programs. To combat this, and any possible legal action against themselves, they provide a disclaimer that pops up when their email monitoring programs are installed. One example of such a disclaimer reads:

\begin{quote}
Before using any of our products, documentation and web site(s), you must understand that under some circumstances and under certain legal conditions your use/misuse of the software can lead you to a court (a legal action can be taken against you). Make sure using our software does not interfere with your local laws. You must understand that if your actions will be classified as intruding on third party privacy, you will be the only person responsible for this... The United States Department of Justice recommends that a banner notice giving [sic] clear and unequivocal notice to intruders that by signing on to the system, they are expressly consenting to having
\end{quote}

\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} One example of this is the KeyGhost Keylogger device, http://www.keyghost.com (last visited Nov. 21, 2005).
\textsuperscript{58} One example of this is the Beyond Keylogger program, http://www.supremtec.com (last visited Nov. 21, 2005).
\textsuperscript{59} Wesche, supra note 3, at 106.
III: FEDERAL AND COMMON LAW ELECTRONIC PRIVACY PROTECTION

As is often the case in the legal arena, this dispute over the propriety of email monitoring frequently leads to lawsuits. When an employee decides to sue an employer for an invasion of privacy, the employee can sue under the Federal Wiretap Act,\(^\text{61}\) or the common law tort of invasion of privacy.\(^\text{62}\) The basis of each of these sources of liability lies in the aforementioned right to privacy.\(^\text{63}\)

The constitutionally protected right to privacy was derived from the penumbra of other protections found in the Bill of Rights.\(^\text{64}\) Such rights, however, generally cannot be enforced against non-governmental entities.\(^\text{65}\) The privacy right at issue from illicit monitoring of email can possibly be proscribed by the Fourth Amendment itself, without any need to attach to the penumbras of privacy protections. The Amendment states in pertinent part "[t]he right of the people to be secure in their persons, houses, papers, and affects, against unreasonable searches and seizures, shall not be violated."\(^\text{66}\) This Fourth Amendment prohibition against unreasonable searches and seizures serves as a launching pad for any complete discussion of one’s rights in relation to interception of messages from email systems. Although this analysis applies to a public employer,\(^\text{67}\) the same tests utilized by the Supreme Court in Fourth Amendment cases are used to resolve email monitoring issues in the

---

60. This disclaimer appears when the Family Keylogger program is installed. The disclaimer is available at http://www.spyarsenal.com/disclaimer.html (last visited Nov. 21, 2005).
63. See supra notes 7-11 and accompanying text.
66. U.S. Const. amend. IV.
context of the private workplace. These tests will be used to analyze the current state of the law with regards to both the federal statute and the common law tort.69

There is some degree of privacy possessed by employees in the workplace. Some states have codified the privacy right or provided for the right in their state constitution. The courts have, in varying degrees, found that privacy does exist in the private workplace.70 In order to prevail in a suit for violation of those rights, the plaintiff must prove that they had a reasonable expectation of privacy in the space or materials that were invaded.71 There is a significant question regarding the privacy, or lack thereof, of an employee's personal email communications sent, received, and stored at the workplace.72 Employees in the public sector enjoy a degree of privacy granted to them by way of the Fourth and Fourteenth Amendment protections against unreasonable searches and seizures. The United States Supreme Court announced in O'Connor v. Ortega that public employees enjoy a degree of privacy that is tempered by variations in each employment relationship, and the degree of privacy that each particular environment can afford is evaluated on a case-by-case basis.73 Private employees, however, are protected by the Electronic Communications Privacy Act of 1986 (ECPA), which authorizes civil as well as criminal sanctions for those who intentionally access email services without authorization or in excess of their authorization.74

The ECPA not only protects the privacy of employee email communications, but results in the privacy of all wire and electronic communication in the United States being governed by federal statute. In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act, commonly known as the Federal Wiretap Act.75 The purpose of this Act was to protect individual privacy by limiting the

69. See infra Part IV.
73. 480 U.S. at 709.
74. Wesche, supra note 3, at 109-110.
circumstances by which the interception of communications may lawfully take place.\textsuperscript{76} The Wiretap Act was created soon after the Supreme Court overturned a New York wiretapping statute by declaring it unconstitutional in violation of the Fourth Amendment right to privacy.\textsuperscript{77} Congress drafted the Wiretap Act with the instructions of the Court in the forefront of their minds.\textsuperscript{78} Its statutory framework was designed to satisfy the Court’s strict requirements for surreptitious surveillance so as not to violate anyone’s Fourth Amendment right to privacy.\textsuperscript{79} Although it was primarily intended to address government wiretaps, the 1968 Act applies to private individuals and employers as well.\textsuperscript{80} Eighteen years later, in reaction to technological advances, the ECPA amended the 1968 Act.\textsuperscript{81} The ECPA added protection against the unlawful interception and disclosure of electronic communication to the existing protection of wire and oral communication.\textsuperscript{82} It also proscribed the unlawful access and disclosure of electronically stored wire and electronic communications under Title II of the ECPA, commonly known as the Stored Communications Act (SCA).\textsuperscript{83}

Despite their obvious importance, the statutes remain poorly understood. Courts, legislators, and legal scholars alike have had a very hard time making sense of these federal statutes.\textsuperscript{84} They are dense and confusing, and the two sections of the amended Federal Wiretap Act, at times, seem to contradict or diminish the use of one another.\textsuperscript{85}

\begin{itemize}
\item 77. Berger v. New York, 388 U.S. 41 (1967) (Although the case holding was later overturned, the act was created to fit within the court’s framework of searches and seizures, and the reasons for creating the statute did not change).
\item 78. \textit{Id.} at 56.
\item 79. Supplemental Brief for of Amicus Curiae The Center for Democracy and Technology, et al. as Supporting United States at 1, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383).
\item 80. Baum, \textit{supra} note 9, at 1022 n. 55-58.
\item 82. Title I of the ECPA, 18 U.S.C. §§ 2510-2522 (2002).
\item 83. 18 U.S.C. §§ 2701-2711 (2002).
\item 84. \textit{See, e.g.}, United States v. Councilman, 418 F.3d 67, 84 (1st Cir. 2005); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998). Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Dixon, \textit{supra} note 21.
\item 85. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877-79 (9th Cir. 2002); \textit{Id.} at
result of the current incarnation of this act, the statute has been called a "skein of statutory opacity." This uncertainty has made it difficult for legislators to legislate in the field, reporters to write about the law, and scholars to offer guidance in this very important area of law. Federal circuit courts have called the Wiretap Act, "complex," "convoluted," and "ambiguous."

Email messages exist in formats covered by both the ECPA and SCA, depending on whether the email messages are being sent between parties or stored for backup purposes. Thus, email messages are protected by different sections of the ECPA depending on their purpose at any particular time. A message that is first being sent from one party to another is protected under Title I of the ECPA, whereas a message that has already been read and is being stored for later viewing is protected under Title II, the SCA. This conflict between the ECPA and the SCA has led to much conflict in the courts, leading to many heated dissents.

Oddly enough, until very recently, there was a consensus with regard to how to apply the differences between the two statutes. After a recent en banc decision of the United States Court of Appeals for the First Circuit, overturning a panel decision rendered in the same case, the entire matter is once again fraught with vagueness.

As noted in a law review comment on the topic, "[a]lthough the ECPA does not directly mention email, the Act's legislative history

86. Finkin, supra note 28, at 478.
88. Smith, 155 F.3d at 1055.
89. Id.
90. See Councilman, 418 F.3d at 84.
91. Konop, 302 F.3d at 888-92 (Reinhardt, J., dissenting).
92. Id. at 888.
93. See Councilman, 418 F.3d at 85-90 (1st Cir. 2005) (Torruella, and Cyr, J.J. dissenting); see also Konop, 302 F.3d at 888-92 (Reinhardt, J., dissenting).
94. Compare Councilman, 418 F.3d at 84 (disagreeing with other courts regarding temporary storage), with United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004) vacated, 418 F.3d 67 (1st Cir. 2005) (agreeing with other courts regarding temporary storage).
95. Councilman, 418 F.3d 67.
96. See infra notes 154-65 and accompanying text.
makes it clear that e-mail is included within the ECPA’s definition of electronic communication.”97 This is exhibited in the statements made in the Senate in consideration of the amendments made to the ECPA in 1986:

Tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.

The law must advance with technology to ensure the continued vitality of the Fourth Amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.98

The key provisions of the ECPA state, “[a]ny person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished.”99 While these provisions, by themselves, would appear to prohibit employer monitoring of employee email, the ECPA contains three key exceptions that allow employers to monitor employee communications. These three exceptions are: the business use exception,100 the service provider exception,101 and the consent exception.102 The courts have added a fourth exception to ECPA liability that requires the interception of the communication be

102. Id. at § 2511 (2)(d).
contemporaneous with the transmission of the communication. These four exceptions will be analyzed in greater detail when they are applied to specific circumstances of email monitoring.

The other path that employees can pursue while seeking to sue their employer is to bring a lawsuit under the tort entitled invasion of privacy. The common law offense of invasion of privacy can be violated by one of four distinct invasions into the private life of an individual. "Of these four, the tort commonly called unreasonable intrusion upon the seclusion of another appears to be the most applicable to email monitoring." The Restatement (Second) of Torts reads, "[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."

To prove this common law claim for invasion of privacy, a plaintiff must satisfy two separate and distinct requirements. First, the plaintiff must show that a reasonable expectation of privacy existed. Second, the plaintiff must show that there was a highly offensive invasion of that privacy. In order to fulfill the first requirement, to prove a legitimate expectation of privacy, a plaintiff must show that their subjective expectation of privacy is one that society accepts as objectively reasonable. After the court has established there has been an invasion, the court must determine whether the invasion was "highly offensive."

103. See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994); but see United States v. Councilman, 418 F.3d 67 (2005) (holding that email that is in storage can be intercepted for the purpose of liability under the Wiretap Act).

104. See infra Part III. The Electronic Communication Privacy Act and the Stored Communications Act were further amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, the USA PATRIOT Act. The PATRIOT Act, however, did not substantially affect the subsections of the Wiretap Act that are relevant to the topic at hand.


107. Beeson, supra note 97, at 209.


Before any court had an opportunity to examine privacy in the context of email, the Third Circuit commented on the applicability of the tort of intrusion upon seclusion to an employer reading the personal, postal mail of an employee. In *Vernars v. Young*, a corporate officer, without authority to do so, opened and read postal mail that had been addressed and delivered to another Vernars employee and, moreover, had been plainly marked "personal." The court held that the action of the employer constituted an intrusion upon seclusion. This case implies that a common law right to privacy may exist in one's personal mail, fulfilling the first requirement of the Restatement. From the language the court uses, it seems clear that this expectation of privacy in one's personal mail would be reasonable, thus fulfilling the second requirement of the Restatement. However, the courts have not extended the right to privacy as expressed in *Vernars* to cover email, despite the similarities between email and postal mail.

The employee's choice of law and decision of what doctrine to sue under may be based on what kind of email was monitored and how the monitoring took place. There are two classes of email that are used in the corporate environment and are pertinent to the privacy analyses: company email accounts and web-based, personal email accounts. Company email accounts are meant for internal company communications and for communications with a company's clients. While it may be a company's intention that their email system only be used for company purposes, the email system itself will not prevent personal email from being sent, even if there are corporate policies preventing such use. Company accounts are accessed by using software that is specifically installed for this purpose, such as Microsoft Outlook or Exchange and Novell GroupWise. One example of such an email account is BillGates@microsoft.com. The company email systems are managed by email servers, to which the employer has complete

113. 539 F.2d 966 (3rd Cir. 1976).
114. *Id.* at 968.
115. *Id.* at 969.
117. *Vernars*, 539 F.2d at 969.
120. This is a fictitious email address. Most large companies have their own email domain and their own email servers servicing the email accounts.
access to view all incoming and outgoing email. All email sent using the company email system is saved on the company server even after an employee deletes the email from their account.

Web-based, personal email accounts are accessed through the Internet using any commercially available web browser such as Internet Explorer, Netscape, or Opera. If an employer provides Internet access through its network, the employees may access a web-based, personal email account from any workplace computer. The major difference between the web-based form and company email “is that e-mails sent and received by the web-based personal accounts are not automatically stored on the company server.” Email is instead stored on the email provider’s servers at an offsite location. No one in the employee’s company has access to the employee’s stored web-based personal email. This form of email is not routinely saved to the employee’s computer, and therefore the employer can not view the email by accessing the computer that the employee works with.

IV: WHAT COURTS SAY ABOUT EMPLOYER LIABILITY FOR PRIVACY VIOLATIONS

A. Monitoring Employee Corporate Email Accounts

The next step in evaluating employer liability for the monitoring of employee email is to analyze how the ECPA and the Restatement apply to the two categories of email. In order to understand how the courts have analyzed the email privacy questions, one must keep in mind that many companies have implemented corporate email policies. These policies give notification to employees that their email will be monitored and require the employee to consent to the monitoring. The consent of employees to be monitored, or the lack of consent, is a major factor the courts use in determining employer liability for email monitoring.

When an employee has consented to monitoring of their email, courts have overwhelmingly ruled in the employer’s favor when the employer has monitored the employee’s use of a company email

121. Echols, supra note 45, at 277.
122. See infra note 265 for an example of such a policy.
account. In applying the Restatement standard, the key issue is whether there is a reasonable expectation of privacy, which is "an objective entitlement founded on broadly based and widely accepted community norms, and the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant."  

The nature of the workplace is generally a public one, and an employee is hired for the purpose of furthering company business and not to attend to personal matters. It should be expected that all use of the tools that the employer provides should be for company business, and any use of such tools should not carry any expectation of privacy. Predictably, employer provided tools should be restricted to use for company business. These tools should not carry any expectation of privacy.

Another reason the courts give for the diminished expectation of privacy is that emails can be forwarded to anyone. The original sender of an email may think that their words are private and will only be read by the intended recipient, but this is not true because the recipient can forward the email to any number of people. Although the sender’s intentions were that only the recipient read the email, the sender knows or should know of the possibility that the email can be forwarded to anyone. There can be no expectation of privacy in such a communication that can be instantaneously sent to anyone that has access to an Internet connection.

Email transmissions in many ways are no different than older forms of communication. For example, when one sends a letter in the mail via the United States Postal Service and addresses it to a certain person, the sender has a reasonable expectation of privacy in that letter. The sender believes that no one but the addressed recipient will read the letter. However, once the letter is received by the intended recipient, the recipient may do as they please with the letter. The recipient can post it wherever they want, and may show it to whomever they choose. Similarly, an email message, once it is received, can be copied, posted or

127. Id.
forwarded, but with much greater ease than with traditional mail. As a result of the control the recipient of any mail or email message has, the sender cannot retain any expectation of privacy with the message once it is in the hands of the recipient.128

The courts have ruled that employees have no reasonable expectation of privacy for communications transmitted over an employer’s email system.129 One reason the courts give for allowing employer monitoring of employee email is that the employers are unlikely to abuse their monitoring privilege.130 The courts reasoned that it is in the employer’s best interest to balance surveillance needs with employee quality of life.131 Another reason that employers will not likely abuse their privilege is that employer misuse of personal information is prohibited by a variety of existing legal doctrines.132 Courts have also noted, however, that even if there was some expectation of privacy in the employee’s email, it is outweighed by the employer’s interests in preventing inappropriate or illegal activity.133 In such a case, the invasion of privacy would not pass muster of the second requirement of the Restatement, that the invasion be “highly offensive.”134

With regard to the second requirement of the Restatement, that the invasion be highly offensive, the courts have applied the same reasonableness test that they apply to the first requirement of the Restatement.135 In fact, courts use the exact same reasons to show that the invasion is reasonable as they use to prove that the invasion is not offensive.136 There are no novel explanations as to why an unreasonable invasion of privacy in an email context would not be highly offensive. Courts simply restate the arguments for the invasion not being unreasonable, and change the words to fit into the offensiveness

128. Id.
129. See, e.g., Id.
130. Fazekas, supra note 36, at *26-27.
131. Id.
132. Id. at 28.
135. See id.
requirement.\textsuperscript{137} If the facts in a case show that the monitoring constitutes an invasion of privacy according to a reasonable person, then the courts would be hard pressed to skew the justifications that did not work in the employer's favor in the first Restatement requirement to fall on the employer's side with respect to the second requirement of the Restatement. This may account for the reason that so few cases proceed past the first hurdle of proving that the invasion was offensive to a reasonable person. What it seems from the courts' analyses is that if it is a reasonable invasion, it is necessarily not highly offensive, and if it is highly offensive, then it is probably not a reasonable invasion of privacy.\textsuperscript{138}

Notice and consent can also be bars to a tort claim against an employer. When an employer gives notice to an employee that email may be monitored, this "undermines the reasonableness of an employee's claim that he or she believed such information was private and not subject to search."\textsuperscript{139} In such an instance, "the employee [would have been] explicitly cautioned that information flowing through or stored on computers within the network cannot be considered confidential, and . . . that network administrators and others were free to view data downloaded from the internet."\textsuperscript{140} There is also a separate, but related theory as to why employers are allowed to monitor employee emails. It would be counter intuitive to hold that an employer should be liable for illegal acts committed by employees through the use of email by relying on the doctrine of respondeat superior, without providing the employer with the legal means to monitor the email that can cause them to be liable.\textsuperscript{141}

In order to analyze the situation where an employer monitors a company email system with the consent of the employees, the four exceptions to the ECPA must be individually applied. If an employer falls into any of these four exceptions, the employer is exempt from

\textsuperscript{140} Id.
\textsuperscript{141} See Echols, \textit{supra} note 45, at 295-298.
liability for the interception of an employee’s email; however, it is still beneficial to analyze all four exceptions. The first exception to the ECPA is the business use exception.\textsuperscript{142} The exception states that any equipment or component used in the ordinary course of business is not considered an electronic device for the purpose of the statute.\textsuperscript{143} As a result of the component not being considered a device, an employer who uses such a tool to monitor an employee is not liable under the ECPA.\textsuperscript{144} A company email system is such a business tool.

The second exception to the ECPA is the service provider exception. This provision states that “[i]t shall not be unlawful . . . for . . . an officer, employee, or agent of a provider of wire or electronic communication service . . . to intercept . . . that communication in the normal course of his employment.”\textsuperscript{145} In situations where an employee is using the company, proprietary email system, the employer is the service provider of the “electronic communication service,” which places the employer squarely within the confines of the service provider exception to the ECPA.\textsuperscript{146}

Consent is the third exception to the ECPA. The statute provides that, “[i]t shall not be unlawful under this chapter for a person . . . to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception.”\textsuperscript{147} In such an instance where an employer is monitoring a company email system, there is written or implied consent from the employee who is “one of the parties to the communication.”\textsuperscript{148} Therefore, the employer will be exempt from liability under the ECPA. However,

\begin{itemize}
\item even if an employer can successfully establish that the monitoring of employee communications was expressly or impliedly consented to, an employee may still be able to prevail if he or she establishes that the employer had a criminal or tortious purpose for conducting the monitoring. This “tortious purpose” must be more than an
\end{itemize}

\begin{footnotes}
\item \textsuperscript{142} See 18 U.S.C. § 2510 (5)(a) (2002).
\item \textsuperscript{143} Id.
\item \textsuperscript{144} Id. § 2511 (1) (2002).
\item \textsuperscript{145} Id. § 2511 (2)(a)(i) (2002).
\item \textsuperscript{146} See McIntosh, supra note 81, at 549-553 for a further discussion on the applicability of the business use exception to email monitoring.
\item \textsuperscript{147} Id. § 2511 (2)(d).
\item \textsuperscript{148} Id.
\end{footnotes}
employer's mere intent to surreptitiously record a conversation. For instance, extortion, blackmail, and causing emotional distress are examples of such tortious purposes. In addition, even if some lawful purpose exists to justify the interception, there may still be a tortious or otherwise unlawful purpose behind the interception that would take it out of the Consent Exception.149

The last exception to the ECPA is the court-added contemporaneity requirement. In *Steve Jackson Games, Inc. v. United States Secret Service*, the Fifth Circuit was one of the first courts to hold that for an employer to be in violation of the ECPA, the employer must intercept the email at the time of transmission.150 Nearly every court that has subsequently decided the issue has agreed with the Fifth Circuit that to be in violation of the ECPA, the interception must be contemporaneous with the transmission of the email.151

The Ninth Circuit, for example, held in *Konop v. Hawaiian Airlines* that this definition is consistent with the intent of the ECPA, which created the Stored Communications Act for the express purpose of addressing access to stored electronic communications.152 The vigorous dissent in *Konop* argued that the term “intercept” cannot possibly mean that the interception must be contemporaneous with transmission.153 The dissent contended that such a requirement would render the ECPA toothless and completely destroy any value of the SCA.154

The dissent in *Konop* based its assertions on the premise that *Steve Jackson Games* was rendered somewhat obsolete by the growth of the Internet, a phenomenon that the Fifth Circuit judges deciding that case could not have meaningfully incorporated into their reading of the statute.155 In particular, it would have been impossible to anticipate the expectations of privacy that people would develop regarding the Internet, expectations that are crucial to interpreting the statutory scheme consistent with Congressional intent to protect privacy interests.156 Still, nearly every court has agreed with the majority in *Konop* that to be in

149. McIntosh, *supra* note 81, at 557.
150. 36 F.3d 457, 459 (5th Cir. 1994).
151. *See, e.g.*, *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002).
152. *See id.* at 878-79.
153. *See id.* at 886-87.
154. *See id.* at 887-89 (Reinhardt, J., dissenting).
155. *See id.* at 889.
156. *See id.* at 890-91.
violation of the ECPA, the interception must be contemporaneous with the transmission.\textsuperscript{157} In cases of employer controlled systems, the interception is never contemporaneous with the transmission because the employer intercepts the email as soon as it enters the company email system, but after the transmission of the email and well before the email reaches the recipient. Given this procedure, an employee will never have a federal cause of action against an employer for email that is monitored through a company email system.

In a recent decision, the First Circuit disagreed with every other circuit court on this topic.\textsuperscript{158} The \textit{Councilman} opinion reads very similar to the dissent in \textit{Konop.}\textsuperscript{159} In \textit{Councilman}, the First Circuit disagreed with the interpretation that the other circuit courts gave to the legislative intent of Congress when they created the ECPA.\textsuperscript{160} The First Circuit held that “Congress had in mind these types of pre- and post-transmission ‘temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,’ when it established the definition of ‘electronic storage.’”\textsuperscript{161} The court reasoned that Congress did not mean to exclude the type of temporary storage that a message goes through during its transmission from the scope of the ECPA.\textsuperscript{162} Consistent with the dissent in \textit{Konop}, the \textit{Councilman} court did not believe that Congress intended that an email message, while in transit from the sender to the recipient, switches back and forth between ECPA protection and SCA protection.\textsuperscript{163} The court stated that “we doubt that Congress contemplated the existential oddity that Councilman’s interpretation creates: messages . . . briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again.”\textsuperscript{164} In sum, the court rejected the accepted distinction that email messages cease to be an “electronic

\textsuperscript{157} See, e.g., Theofel v. Farey-Jones 359 F.3d 1066, 1077-78 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F. 3d 107, 113-14 (3rd Cir. 2003); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994).

\textsuperscript{158} See Councilman, 418 F.3d 67 (1st Cir. 2005).

\textsuperscript{159} See Konop, 302 F.3d at 887-91 (Reinhardt, J., dissenting).

\textsuperscript{160} See United States v. Councilman, 418 F.3d 67, 72-77 (1st Cir. 2005).

\textsuperscript{161} Id. at 77 (quoting the language of the ECPA, 18 U.S.C. § 2510(17)) (internal citations omitted).

\textsuperscript{162} Id.

\textsuperscript{163} Id. at 78.

\textsuperscript{164} Id.
communication” during the “momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage.”

The court in Councilman held that email in temporary storage can still be intercepted; therefore, the email need not be “in transmission” to fall under the ECPA. While it may seem as though the court was doing away with the contemporaneity requirement, the court stated unequivocally that “we [] need not decide that question,” whether the interception needs to occur contemporaneously with the transmission. The court did hint that it wanted to do away with the contemporaneity requirement when it said that it was not “prepared to recognize a contemporaneity or real-time requirement,” however, the Councilman court was simply not clear about what it wanted the decision to mean for any future sets of facts that may arise. The court may have tried to clarify the law with respect to email interception, but they failed to do so.

The analysis for email monitoring on an employer system without the consent of the employee is much the same analysis as for monitoring with employee consent. The only difference in the Restatement analysis is that there is no reduction of the expectation of privacy due to consent to being monitored. When there is no employee consent, the legal rules are not clear. “[W]here [an] employer has no policy notifying employees that their computer use could be monitored, and there is no indication that the employer directs others to routinely access the employees’ computers, the employees’ subjective beliefs that their computer files are private may be objectively reasonable.” However, an organization that has a company handbook notifying employees of an email monitoring scheme will escape liability for such monitoring. One example of such a company handbook is that of U.S. Bancorp,

165. See id. at 79.
166. Id. at 70.
167. Id. at 80.
168. Id. (stating “[w]e note, however, that even were we prepared to recognize a contemporaneity or real-time requirement—a step that we do not take today—we think it highly unlikely that Councilman could generate a winning argument in the circumstances of this case.”).
discussed in Thygeson v. U.S. Bancorp.\textsuperscript{171} The handbook stated that "U.S. Bancorp reserves the right to monitor any employee's email and computer files for any legitimate business reason."\textsuperscript{172} Regardless of whether an employee subjectively believes that emails will be private, such a belief is not objectively reasonable after the employee is notified by an employer that email will be monitored.\textsuperscript{173}

Some courts have even gone so far as to say that with regard to a company, proprietary email system, the employer may monitor email even when the employees have been assured that all email communications would remain confidential.\textsuperscript{174} In Smyth v. Pillsbury, the employer repeatedly assured its employees that email communications would not be intercepted.\textsuperscript{175} Even with these clear and obvious statements, the court still held that employee Smyth had no cause of action for invasion of privacy.\textsuperscript{176} Smyth's reasonable expectation of privacy, combined with the offensiveness of the invasion, did not outweigh the company's interest in self protection.\textsuperscript{177} The court concluded that "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its email system outweighs any privacy interests the employees may have."\textsuperscript{178} Even without the consent of the employee, employers are free to monitor employee email without any fear of liability under the Restatement when they are monitoring their own email systems.

As seen in Smyth, when an employee relies on a company policy that is supposed to protect them from invasions of privacy, the result may not be what they expected. However, in some jurisdictions, reliance on a company policy that is clearly spelled out in a personnel manual can protect an employee from an unwarranted invasion by their employer. Such is the law in Massachusetts, where this type of written company policy could be enforced against an employer as an express contract.\textsuperscript{179} An intrusion into the privacy of an employee in violation of

\begin{itemize}
  \item \textsuperscript{171} Id.
  \item \textsuperscript{172} Id. at *20.
  \item \textsuperscript{173} Id.
  \item \textsuperscript{175} Id. at 98.
  \item \textsuperscript{176} Id. at 101.
  \item \textsuperscript{177} Id.
  \item \textsuperscript{178} Id.
  \item \textsuperscript{179} Wesche, \textit{supra} note 3, at 114.
\end{itemize}
this written company policy could give rise to a claim for breach of contract.\textsuperscript{180} Such a provision could cause an employee to have a reasonable expectation of privacy, a prerequisite to a cause of action under the common law invasion of privacy tort. In other states where the breach of contract claim does not arise from the company policy, employers may be able to ignore their own policies prohibiting email monitoring, with no recourse to their employees beyond the exception filled ECPA remedies.\textsuperscript{181} "Reliance in good faith on the policy may not be sufficient to protect employee privacy."\textsuperscript{182}

Another reason for employers' apparent freedom to monitor email is that "[o]nce [a] plaintiff communicated... over an email system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."\textsuperscript{183} The Smyth court holding heavily weighted the fact that the email was voluntarily sent, and such communications have no privacy interests.\textsuperscript{184} In analyzing the second prong of the tort of invasion of privacy, namely that the invasion be highly offensive, the court relied on the same grounds for dismissing the plaintiff's claim.\textsuperscript{185} Following reasoning similar to what they had used to decide there was no invasion at all, the court opined that since the plaintiff voluntarily sent the email, any invasion into such communication is not highly offensive.\textsuperscript{186} Once again,\textsuperscript{187} the court blurred the line between the two requirements of the Restatement, that there is an invasion of privacy and that such an invasion is highly offensive. According to the Restatement, once a court decides that there is no invasion of privacy, then there need not be a discussion whether the invasion was highly offensive.\textsuperscript{188} Nevertheless, courts tend to analyze the second prong even after they decide that the first requirement of the Restatement was not met.\textsuperscript{189} Perhaps courts are not

\begin{footnotesize}
\begin{itemize}
\item[180.] \textit{Id.}
\item[181.] \textit{Id.}
\item[182.] \textit{Id.}
\item[184.] \textit{Id.}
\item[185.] \textit{Id.}
\item[186.] \textit{Id.}
\item[187.] For another instance of the court blurring the lines, see supra notes 135-138 and accompanying text.
\item[188.] Restatement (Second) of Torts § 652B (1977).
\item[189.] \textit{See, e.g.,} Smyth 914 F. Supp. at 100-01.
\end{itemize}
\end{footnotesize}
comfortable relying on nullifying one requirement alone because the reasoning and logic applied to both requirements is flawed and out of touch with modern technology.

In a minority of cases where employees have been notified of monitoring, courts have held that there is still a reasonable expectation of privacy. In *Haynes v. Office of the Attorney General Phill Kline*, the United States District Court for the District of Kansas ruled that the plaintiff had successfully demonstrated a subjective expectation of privacy and raised serious issues concerning whether this expectation of privacy was objectively reasonable.\(^{190}\) In that case, there was some evidence of notification: every day a policy was displayed on the computers in the Attorney General’s office. The policy read, in part: “[t]here shall be no expectation of privacy using this system.”\(^ {191}\) This screams notification loud and clear. The court, however, employed a balancing test to consider the policy against oral representations made by employees of the Attorney General to the plaintiff.\(^ {192}\) The court held that the facts, taken as a whole, suggested that the plaintiff’s expectation of privacy was objectively reasonable.\(^ {193}\) The other factors that the court considered were that employees are allowed to use their work computers for private communications; employees are told how to create ‘public’ and ‘private’ files; employees are advised that ‘intentional access to another user’s email without permission’ is prohibited; employees are given passwords to prevent others from gaining access to their computers; and there was no evidence that any AG official had ever monitored or viewed any private files, documents or emails of any employee.\(^ {194}\)

The approach is logical, yet novel, and it has not been followed by any other court when dealing with a company email system. Following such an approach would provide a well balanced test, weighing the values of the rights of employers and employees in each individual case. However, as it now stands, this is not the practice followed in most

\(^{191}\) *Id.* at 1162.
\(^{192}\) *Id.* at 1161-62.
\(^{193}\) *Id.*
\(^{194}\) *Id.*
courts.\textsuperscript{195}

The ECPA provides additional requirements against which non-consensual email monitoring must be tested.\textsuperscript{196} As under the Restatement, the analysis of non-consensual email monitoring is similar to the analysis where the employer has obtained consent from the employee. Under both circumstances, the ECPA recognizes that an employer may avoid liability by meeting any of the exceptions regarding business use, service provider, and contemporaneity. Courts are split, however, on how to approach situations where express consent has not been obtained from the employee.\textsuperscript{197} Case law has established that under U.S.C. § 2511(2)(d), consent may be either express or implied.\textsuperscript{198} Courts have explained implied consent by analogizing the sending of email to leaving a message on an answering machine.\textsuperscript{199} When one leaves a message on an answering machine or a voice mail system, the caller knows that the message was saved on the machine and can be permanently archived. Similarly, in the email context, the sender knows that the nature of sending an email is that a record of it can be downloaded, printed, saved, and stored on the company email system. Accordingly, by the act of sending an email via the Internet, the sender "expressly consents by conduct to the recording of the message."\textsuperscript{200} However, the Court of Appeals for the Eleventh Circuit mentioned that such consent "is not to be cavalierly implied."\textsuperscript{201} Because courts have diverging decisions on the issue, it is unclear whether the consent exception would be applied in the context of an employer that monitors the company email system without the express consent of its employees. Nevertheless, the other three ECPA exceptions would apply and would exempt an employer from liability.

The consent exception under the ECPA represents perhaps the most


\textsuperscript{198} Watkins, 704 F.2d at 581.

\textsuperscript{199} Proetto, 771 A.2d at 830.

\textsuperscript{200} Id.

\textsuperscript{201} Watkins, 704 F.2d at 581.
fair of the four exceptions to employer liability for employee monitoring. The exception focuses on the employer’s conduct informing employees about workplace monitoring and the employee’s express or implied consent to such monitoring. It also permits the imposition of liability on an employer that otherwise meets the exception’s requirements if the employer has acted with a criminal or tortious purpose.\(^\text{202}\)

Evaluating the employer’s purpose for monitoring ensures that, to the extent employees surrender some of their privacy rights because of the realities of the workplace, the employer cannot improperly use information gathered as a result of monitoring. Conversely, an employer who has provided adequate notice of the occurrence and extent of monitoring activity will not be liable for such monitoring, unless the monitoring is conducted with a criminal or tortious purpose.\(^\text{203}\)

Thus, the consent exception achieves the greatest balance of rights among the ECPA exceptions because its applicability is conduct dependent. “Given the large percentage of employers who now inform their employees of monitoring activity, use of this exception by employers should increase.”\(^\text{204}\)

The Kraslawsky court, on the other hand, viewed consent only “as a factor in the balancing analysis, and not a complete defense to a privacy claim[,]”\(^\text{205}\) but that case dealt with an invasion that was far more offensive than reading an individual’s email. Instead, Kraslawsky involved forcing employees to take drug tests and the termination of an employee for failure to take the test.\(^\text{206}\) When an employer requires drug testing as a condition of employment, the employee must either agree to the invasion of privacy or lose their job, whereas in our line of cases, “[w]hen an employer requires consent to email monitoring, the employee . . . can avoid any invasion of [their] privacy by using [the] computer for business purposes only, and not for anything personal.”\(^\text{207}\)


\(^{203}\) McIntosh, supra note 81, at 577.

\(^{204}\) Id.


\(^{206}\) Id. at 182.

Following this logic, in the context of an email monitoring case, consent would be a complete defense to an invasion of privacy claim. When the traditional privacy analysis is applied to the practice of monitoring web-based, personal email accounts in the workplace, employers do not have as strong a legal position as they do when monitoring company, proprietary email accounts.

The seminal case that discusses monitoring of web-based, personal email accounts is *Fischer v. Mount Olive Lutheran Church.* In this case, the employer, Mount Olive Lutheran Church, through its agent, Defendant Connor, accessed the plaintiff's Hotmail email account without notice, consent, or authorization. The court opined that the legislative history of the Federal Wiretap Act showed that Congress intended the Act to cover this situation of email monitoring. For support, the *Fischer* court quoted an example from the legislative history of the act:

For example, a computer mail facility authorizes a subscriber to access information in their portion of the facilities storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of the act. Similarly, a member of the general public authorized to access the public portion of a computer facility would violate this section by intentionally exceeding that authorization and accessing the private portions of the facility.

The *Fischer* case is the only decision on this issue of an employer monitoring an employee's web-based email. The court did not provide a full discussion on the merits of the plaintiff's case and did not go into detail about how the various exceptions to the ECPA would apply to an employer monitoring an employee's web-based email account. Accordingly, we do not yet have a court decision that specifically discusses how the ECPA exceptions will apply to this form of email monitoring.

The court in *Fischer* applied 18 U.S.C. § 2701 of the Stored

---

208. 207 F. Supp. 2d 914 (W.D. Wis. 2002).
209. *Id.* at 921.
210. *Id.* at 926.
211. *Id.*
Communications Act (SCA)\textsuperscript{212} to a webmail monitoring context and thus provided some statutory guidance. The court suggested that employers who access employees' email accounts without authority and then proceed to block the employee's access to their own account will be in violation of the SCA provision of intentionally exceeding an authorization to access that facility and thereby obtain, alter, or prevent authorized access to a wire or electronic communication.\textsuperscript{213} If the employer guessed or hacked the password of an employee's web-based email account, the employer would then have access to all of the employee's email. The employer could even view email that the employee himself had not yet viewed, and had no intention of ever viewing in the office. Based on this reading of the \textit{Fischer} opinion, an employer can read email from any email account that an employee has, even if the employee only used that account from the office just one time. The employer would only be liable if they blocked the employee from viewing their own mail. There is no valid justification for an employer monitoring email accounts that are rarely, if ever, viewed in the office.\textsuperscript{214} This type of email does not negatively affect work productivity, or subject the employer to adverse risks; therefore, it should not weigh in favor of the reasonableness of such an invasion of privacy. It seems the court has approached the locked door of one's private email and given the key to employers.

One commentator said of the \textit{Fischer} case that it sets

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 \textit{Fraser}. In summary, while the court leaves unresolved the issue of monitoring webmail, they apparently approve of monitoring web-based, personal email messages accessed from work.\textsuperscript{215}

A major problem with the aforementioned analysis is that there is no difference between "webmail" and "web-based personal, email messages accessed from work" that the commentator refers to. An employer cannot access an employee's web-based email account and

\begin{itemize}
\item \textsuperscript{212} Title II of the Federal Wiretap Act.
\item \textsuperscript{213} \textit{Fischer}, 207 F. Supp. 2d at 926; 18 U.S.C. § 2701 (a)(2).
\item \textsuperscript{215} \textit{Id.} at 140.
\end{itemize}
know which emails were viewed from the office. Therefore, monitoring of webmail must be either legal or illegal. There cannot be a middle ground that permits employers to read only those emails that they think an employee viewed while at work. That situation is illogical and unworkable. Perhaps what the court was implying in Fischer was that email, once it is read and saved on the company computer or server, becomes just like any other computer file that is saved on the computer. However, the ECPA does not apply to such files because there is no communication taking place. The courts agree that no reasonable expectation of privacy exists for the files that are saved on a company computer, thus, a tort claim based on monitoring of files in storage would not stand.\footnote{See supra notes 71-74 and accompanying text.}

After this discussion, it turns out that Fischer does not say much about how the ECPA is applied in the context of an employer monitoring web-based email. Therefore, the question remains as to the law in such a case. While the new monitoring technology may not affect all of the previously discussed factors, employer monitoring may not be justified in every situation and may actually at times impinge on employees’ privacy interests. 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 the invasion of privacy test, whether a reasonable expectation of privacy exists or whether the monitoring would be highly offensive to a reasonable person, has been addressed directly by the courts. At this point, only inferences can be drawn from the courts’ reasoning behind denying the common law claims in the company, proprietary email monitoring cases. Similarities exist between the two email monitoring situations, and many of the same analyses will apply.

\textbf{B. Monitoring Personal Email Accounts}

The analysis of monitoring personal email accounts should begin with the least controversial situation, where the employee has consented to email monitoring. The key Restatement requirement for employer liability is that the employee has a reasonable expectation of privacy.\footnote{See, e.g., Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept 15, 2004); Garrity v. John Hancock Mutual Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002).}
In such an instance where an employee specifically does not use the company email system, but instead uses their own private, web-based email account, one may think that the employee has a reasonable expectation of privacy. The employee took an extra step to protect their privacy by using a personal account, and a reasonable person would most likely believe that there is at least a higher degree of privacy in web-based email used in the workplace than in the company, proprietary email. Intercepting email when it was thought to be private and unreachable is much more offensive than monitoring a company, proprietary email system and cuts against the employer because the employee may have an objectively higher expectation of privacy in their web-based, personal email account.

Of all the factors considered by the courts in weighing the legitimacy of email monitoring, the one that could exclusively justify employer monitoring is the company’s interest in avoiding legal liability. The court in *Booker v. GTE.net, LLC* opined that companies could be held liable on the theory of respondeat superior for unmonitored use of web-based email accounts by employees at work. Therefore, an employer may still be liable for harassing or discriminatory emails sent by employees from their own web-based email accounts if a plaintiff can show that the email was sent from a company computer, using the company’s Internet, on company time, and for a purpose that benefited the employer. Proving benefit to the employer is the most difficult because discriminatory emails do not typically benefit the company. Avoiding legal liability was a factor that favored the employer under the previous analysis but does not lean in either direction under the web-based email analysis.

However, there are still some factors weighing in the employer’s

---

218. See Echols, supra note 45, at 295-298.
219. 350 F.3d 515 (6th Cir. 2003) (discussing the circumstances under which respondeat superior will apply, stating “the critical analysis is whether the employee or agent was acting within the scope of his employment at the time of his tortious act”); Id. at 518 (quoting Osborne v. Payne, 31 S.W.3d 911, 915 (Ky. 2000)). Generally, intentional torts are committed outside the scope of the employment. However, some intentional conduct is so closely related to the employment that it is considered within the scope of employment. The issue of whether an employee’s conduct is within the scope of employment is a question of law.
220. Id. at 518; see also Blakey v. Continental Airlines, Inc., 751 A.2d 538 (N.J. 2000).
favor. Emails can still be forwarded to anyone, and thus employees should have a diminished expectation of privacy. More importantly, the knowledge that the employer is monitoring email, combined with consent to the monitoring, severely curtails any expectation of privacy the employees may have.

When evaluating the second prong of the Restatement, "offensiveness to a reasonable person," inferences also must be drawn from the company email monitoring cases. As with company email monitoring, businesses still have legitimate interests to protect, and presumably employees will be put on notice of possible monitoring if a policy exists. Employees make a calculated choice to have their email monitored by choosing to use the employer's Internet to log on to their personal account. These are some of the factors courts have relied on in holding that a reasonable person would not find the monitoring highly offensive. Because both the monitoring of company systems and web-based email systems share these features,

The courts may reach the same conclusions regarding monitoring of web-based email accounts as they do for company accounts. Therefore, due to the similarity of the characteristics the courts view as important, if employers follow the same procedures as they do when monitoring company email, a valid claim for invasion of privacy would not exist when monitoring personal webmail, so long as it has been accessed from the company's computer and company provided Internet access.

However, the Restatement factors would not weigh as heavily in favor of employers as they do in cases where the employee is using a company email system, so it is unclear how the courts would rule on a claim of invasion of privacy. We must shift the analysis to the ECPA in order to determine if the decision of the courts on a privacy claim would be any clearer.

When dealing with web-based email accounts, the business use exception of the ECPA would not apply because it is meant for

221. See supra notes 126-128 and accompanying text.
222. See supra notes 122-125 and accompanying text.
224. See supra notes 135-140 and accompanying text.
225. Chapman, supra note 214, at 147.
devices that are a basic part of the everyday business proceedings.\footnote{227} One example is a phone extension, something that is built into the phone system and is a necessary part of its day-to-day operation.\footnote{228} In the context of an employer email system, the monitoring aspect is built into the email system and is a basic part of its day-to-day function. However, in the web-based email context, any software that intercepts this type of email is extraneous to the company Internet system and has no necessary purpose for the business other than to monitor email.

Whether the service provider exception\footnote{229} would apply to this type of email monitoring is not clear. The employee is not using the company provided email system but is using the company provided Internet access.\footnote{230} Would the Internet access be enough for the employer to be considered a service provider under the service provider exception and be free from liability for intercepting employee emails? This is another factor that does not clearly favor either side. The consent exception follows the same analysis as that by company email systems and will weigh solely in the favor of the employer.

The last ECPA exception is the requirement that the email be intercepted contemporaneously with the transmission. New spyware technology intercepts emails at the exact moment of transmission.\footnote{231} At the same instant that the recipient views the email, a copy is sent to the employer. Because of the contemporaneous nature of the interception, even the manufacturer has characterized the new software as "almost a wiretap."\footnote{232} This contemporaneous exception has been the downfall of virtually every lawsuit based on the Federal Wiretap Statute. Such

\footnote{227}{See supra note 143 and accompanying text.}
\footnote{228}{See, e.g., Fischer v. Mount Olive Lutheran Church, 207 F. Supp. 2d 914, 921 (W.D. Wis. 2002).}
\footnote{230}{See supra note 145 and accompanying text.}
\footnote{231}{This form of spyware is not to be confused with the common usage of the term with regard to Internet use. Most forms of spyware that people are familiar with keep track of Internet use in order to cause pop up advertisements to appear on the computer that the user is more likely to click. In this note, the term "spyware" refers to programs that are used to spy on the user, without the user's knowledge. The spy programs will not cause any pop ups to appear as they are designed to remain surreptitious at all times.}
technology would now fulfill the contemporaneity requirement of the ECPA, and may finally allow employees a cause of action under the ECPA based on employer monitoring of their email.\footnote{See supra notes 150-168 and accompanying text for a full analysis of the contemporaneity requirement.}

The last situation that must be analyzed is the one that is least favorable to employers, where the employer is monitoring an employee's web-based, personal email without the employee's consent. In the Restatement analysis, the expectation of privacy factors are almost the same as in cases where there is consent. The only difference is the consent analysis because here there is no employee consent.

Possibly, the courts will find implied consent by the employee as they did in \textit{Smyth} and other cases.\footnote{Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996) (holding plaintiff had no "reasonable expectation of privacy" despite the fact that the employer expressly stated the emails would not be intercepted or used against employees. In order to support such a holding the court may have implicitly held that there was implied consent in this case, although the court never mentioned the issue of consent.); see also supra notes 174-178 and accompanying text.} This implied consent, however, is likely to be found only when the email in question involves a company email system because the only cases that courts have ruled consent was implied have involved company, proprietary email systems.\footnote{See, \textit{e.g.}, TBG Ins. Services Corp. v. Zieminski, 96 Cal. App. 4th 443, 450 (Cal. Ct. App. 2002); Garrity v. John Hancock Mutual Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002).} In fact, the employee clearly did not consent when they went out of their way to use a private email system while knowing that the company email system was being monitored. Therefore, it cannot be assumed that general consent to monitor will also cover the web-based, personal email accounts. The spyware that allows monitoring of such personal accounts is a new innovation, with which many employees are not familiar. This type of monitoring, therefore, will most likely require specific consent. As such, absent specific consent to monitor web-based, personal email accounts, an employer quite possibly will face liability for use of the new monitoring technology on these types of email accounts. The case history and statutory interpretations of this type of monitoring are relatively new and undeveloped, so the previously pro-employer legal outcomes are not as certain.

The final analysis is to apply the ECPA exceptions to the web-
based email context. As stated previously, the business use exception, the service provider exception, and the contemporaneity requirement exception may not apply in such a case.\textsuperscript{236} The consent exception would also not apply in this case because courts have never implied consent when they were not dealing with an employer email system.\textsuperscript{237} Therefore, none of the ECPA exceptions would apply to an employer, and an employee may have a cause of action under the federal statute.

What may be gleaned from the various courts’ analyses of the law is that if there is a well designed company policy in place for legitimate purposes, the employer will be able to monitor employees’ web-based email at work. These legitimate purposes would be the same ones that were previously discussed, for example preventing the selling of trade secrets or preventing corporate liability. This company policy would place the monitoring under the consent exception to the ECPA, and remove any tort related expectation of privacy. Moreover, the ECPA only covers interception of electronic communication while in transit.\textsuperscript{238} Companies need only ensure that they are not intercepting the messages, and instead are accessing the email from storage. The Court of Appeals for the First Circuit would disagree with this practice, and allow ECPA liability even if the message is intercepted while in storage.\textsuperscript{239} If employers do intercept the email at the time of transmission as would be the case with the new spyware programs, the question of whether such an action violates the ECPA still remains.

V. STATE APPROACHES TO EMAIL PRIVACY AND PROPOSED LEGISLATION

Since the ECPA exceptions create problems for employees trying to protect their workplace privacy, many states have taken it upon themselves to enact workplace privacy laws. Some states require notice of monitoring. Both Connecticut and Delaware have enacted legislation to require employers to give such notice to employees of their

\textsuperscript{236} See supra notes 226-233 and accompanying text.
\textsuperscript{237} See supra notes 234-236 and accompanying text.
\textsuperscript{238} See supra notes 150-168 and accompanying text.
\textsuperscript{239} See United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (discussing the criminal sanctions of the ECPA. However, the ECPA also allows a private cause of action, and the elements of both criminal and civil actions are identical.); see also supra notes 150-168 and accompanying text.
monitoring policies. These laws do not prevent email monitoring; they merely require notice of the monitoring. However, even the notice requirements are not stringent and are easily fulfilled without much protection or benefit to the employee. Exempted from the notice requirements are "processes that are designed to manage the type or volume of incoming or outgoing electronic mail . . . that are not targeted to monitor or intercept . . . usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and or protection." The problem with this exception is that any email that looks "irregular" can be viewed using the legitimate excuse of computer maintenance, and anything the email contains can be used against the employee as long as the employer can give any valid purpose for viewing the email. The employees in these companies will have no knowledge that their emails are being monitored for any purpose, and may not be careful in keeping their private matters out of the emails they send.

California has attempted to take the lead on this issue with a bill that would require employers to inform employees of their monitoring of email messages. The law would also mandate that employees sign an acknowledgment of receiving notice of the monitoring and allow employees access to information collected about them through monitoring. In 1999, the California bill passed through both houses of the California legislature, but was vetoed by former Governor Gray Davis because of concerns regarding the burden the legislation would impose on employers. Governor Davis asserted that when employees accept employment, they should assume that employers have the right to monitor their electronic communication as a condition of such employment. Like California, several states have debated similar laws, yet none have enacted an employee privacy statute.

Some states have adopted certain provisions of the federal EPCA,

245. Id.
246. See Michael & Lidman, supra note 14.
247. McIntosh, supra note 81, at 559.
while limiting the consent exception, by requiring that both the sender and recipient of an email consent to the monitoring.\(^\text{248}\) This would allow employees much greater freedom in protecting their privacy because even if they consent it will be the rare occasion that the non-employee party to the emails would consent. The scope of state protection under such statutes varies greatly. For instance, states like Nebraska have specifically exempted employers from the provisions of their wiretapping statute, thus providing employees virtually no protections from interception of electronically communicated information.\(^\text{249}\) Still other states, "like Texas, have attempted, though unsuccessfully, to extend protection to employees . . . by proscribing secret electronic surveillance and unreasonable searches."\(^\text{250}\)

Seeking to bring uniformity to the patchwork of inconsistent rules that extend to email, the Notice of Electronic Monitoring Act (NEMA) was introduced with bi-partisan support in both houses of Congress.\(^\text{251}\) NEMA was intended to impose a fair and reasonable check on monitoring activities and afford employees the right to know whether, when, and how their employer is watching them.\(^\text{252}\) Although NEMA is aimed at enhancing employee privacy rights, it does not deprive an employer of the right to monitor. NEMA acknowledges that, while employees should not have an expectation of privacy in email voluntarily sent, stored, or received on the company's system, the employees are entitled to clear notice from employers who choose to exercise their monitoring rights.\(^\text{253}\)

NEMA covers reading employee email, keystroke monitoring, and programs that monitor employee Internet use.\(^\text{254}\) It provides that the requisite notice must be clear, conspicuous, given annually and whenever policies change.\(^\text{255}\) The notice must also specify the frequency

\(^{248}\) Paul E. Hash, E-mail, Electronic Monitoring, and Employee Privacy, 37 S. TEX L. REV. 893, 905 (1996).


\(^{250}\) Settle-Vinson, supra note 35, at 67.

\(^{251}\) See Electronic Privacy Information Center, Workplace Privacy (Aug. 3, 2004), http://www.epic.org/privacy/workplace/default.html (stating NEMA was introduced in 2000 by Democratic Senator Chuck Schumer and Republican Representative Charles Canady).

\(^{252}\) Segarnick, supra note 2.

\(^{253}\) Id.

\(^{254}\) Id.

\(^{255}\) Id.
of the monitoring, the kinds of information likely to be monitored, how
the monitoring will be accomplished, and how the information will be
stored and used.\textsuperscript{256} If an employer engages in secret monitoring in
violation of the notice requirements under the Act, they are subject to
suit for up to $20,000.\textsuperscript{257}

\textbf{CONCLUSION}

A growing number of companies are monitoring both email and
Internet communications of employees. Studies have revealed that more
than three-quarters of major U.S. corporations routinely record and
review employee communications and activities in the workplace.\textsuperscript{258}
These activities include employee telephone calls, email usage and
computer files. The employees often dislike the monitoring and have
repeatedly sued to prevent it, but "[i]n a decade of Internet-related,
workplace privacy cases, private employers have prevailed in every
instance."\textsuperscript{259}

One commentator has astutely written a "word to the wise"
employee: "treat your email systems 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."\textsuperscript{260} The commentator also
advised that one should never send an email from work that you would
be afraid to "read the next day on the front page of a newspaper."\textsuperscript{261}
This warning to employees is very telling of the current state of the law
on the practice of employers monitoring their employees' email. In
addition, employees have yet to win a case brought against an employer
for invading their privacy. There are statutes and common law
principles prohibiting such invasions, but the courts have made the law
in these situations, and the law is simple: employers can monitor the

\textsuperscript{256} Id.
\textsuperscript{257} Id.
\textsuperscript{258} See American Management Association, \textit{supra} note 1.
\textsuperscript{259} Rustad & Koenig, \textit{supra} note 124, at 95.
\textsuperscript{260} Chapman, \textit{supra} note 214, at 152 (quoting Barbara Kate Repa, Computers and
Email on the Job, http://www.hrlawinfo.com/lawguide/Privacy/computers_and_email.asp
(on file with the North Carolina Journal of Law & Technology)).
\textsuperscript{261} Id.
email of their employees as they see fit, with or without the consent of the employees. For their part, employers will continue to monitor the email as long as they feel that it will reduce liability and corporate losses arising from abuses of employee email use.

Courts have made it clear that employers should require specific consent from their employees to monitor both company email accounts as well as web-based, personal email accounts. There should be a company policy that is not merely read and signed by the employee when they begin their employment but should first be actively explained to the employee, and the employee should be reminded of the policy, perhaps often, to prevent any confusion or mistake over the rights of the employee and employer.

Companies should adopt email policies and employee training programs that address these problems and deal with the extent to which company internal and external email is private and secure. They should also deal with the protection of company trade secrets, proprietary information, and confidential information, and avoiding copyright infringement. Most importantly, the policies should make it crystal clear that the users must avoid improper communications that may lead to corporate liability.

Employers do not have to do much to avoid violating the privacy rights of employees. They must weigh the consequences of monitoring their employees email and impinging on their employees' reasonable expectations of privacy with the benefit they receive from such monitoring practices. Employers should ensure that they have legitimate and legally valid reasons before they begin to monitor their employees' email at work. Employers should also "strongly consider whether there are other, less intrusive means to accomplish their objectives before deciding to engage in any kind of electronic surveillance of employees." While this may seem to be an exacting and tough set of requirements placed on the employers, courts have been very lenient in this regard, and have always found that the employers' reasons, however de minimis, were legitimate.

It is hardly surprising, therefore, that employers are told that they

---


263. Id.

264. Id.
should establish a policy for the use of email and the Internet that they require every employee to read and sign.\textsuperscript{265} Employers can diminish an individual employee’s expectation of privacy by clearly stating in the policy that electronic communications are to be used solely for company business, and that the company reserves the right to monitor or access all employee email usage. “An electronic communications policy should [also] include a statement prohibiting the transmission of any discriminatory, offensive or unprofessional messages.”\textsuperscript{266}

Such a policy incorporates notice and consent and removes any expectation of privacy from both company email and web-based email. When the companies require their employees to sign a consent form, the companies should “specifically call out and highlight the fact that the company’s policy will apply to personal web-based e-mail access.”\textsuperscript{267} The policy effectively shuts the door on all privacy related employee lawsuits, and does so in a manner that is respectful to the employees of the company. It is evident that the reasons behind implementing these policies are to help the company and not to harm or harass the employees. This should counteract many of the negative aspects of

\begin{itemize}
\item \textsuperscript{265} The following is an example of an Internet use policy and that can be utilized by an employer, and that includes some of the courts’ recommended language:
\item I, ________, realize that electronic communications are to be used solely for company business, and that the (company name) (hereafter known as “the Company”) reserves the right to monitor or access all employee Internet or email usage. Furthermore, I am fully aware that the Company will keep copies of Internet or email passwords, and that the existence of such passwords is not an assurance of the confidentiality of the communications.
\item This Company also does not tolerate the following:
\item The transmission of any discriminatory, offensive or unprofessional messages.
\item Access to any Internet sites that are discriminatory or offensive.
\item Posting personal opinions on the Internet using the Company’s access, particularly if the opinion is of a political or discriminatory nature.
\item Lastly, I am fully aware that my use of computers in the employment context carries with it social norms that effectively diminish my reasonable expectation of privacy with regard to my use of the company’s computers. Any violation of the above agreement may result in termination of my employment.
\end{itemize}


\begin{itemize}
\item \textsuperscript{267} Chapman, \textit{supra} note 214, at 149.
\end{itemize}
monitoring that employees have complained about.\textsuperscript{268}

Employees in the private workforce currently enjoy no privacy in their electronic mail communications. Even though legal doctrines exist that would seem to recognize a right to privacy for employees, courts have been wary to extend that right very far into the workplace.\textsuperscript{269} As such, private employees have been subjected to monitoring of their email communications in the workplace, and will continue to be subject to such monitoring. Employers believe monitoring of employee email will stem liability for abuses such as corporate espionage and fostering a hostile work environment. At the same time, monitoring hurts the employees because it erodes employee privacy, and creates stress that has a direct negative impact on the emotional and physical health of employees.\textsuperscript{270}

At this juncture, much of the privacy that the Federal Wiretap Act was created to protect has been eviscerated by the realities of modern technology. The statutory language is out of step with the technological realities of advanced computer surveillance and monitoring. The majority of courts, however, do not feel that it is in their province to "graft [new provisions or] meaning onto the statute where Congress has spoken plainly."\textsuperscript{271} This has led to some decisions that may not seem fair, or in tune with the high tech and Internet powered world. The Court of Appeals for the First Circuit in \textit{Councilman} took the realities of modern technology into account when they reached their recent decision.\textsuperscript{272} The court did not believe that Congress intended to perpetuate a toothless statute. While some courts insist that their hands are tied by the existing statute and will remain as such until the law is reformed to address the modern day privacy issues, other courts are now taking proactive steps to help advance these reforms. Perhaps \textit{United States v. Councilman}\textsuperscript{273} will serve as a wake-up call to courts around the nation and cause them to take into account that the Internet has forever changed our cherished right to privacy.

\begin{flushright}
\textsuperscript{268} See supra notes 44-50 and accompanying text.  \\
\textsuperscript{269} O'Connor v. Ortega, 480 U.S. 709 (1987).  \\
\textsuperscript{270} See supra notes 45-47 and accompanying text.  \\
\textsuperscript{271} United States v. Councilman, 373 F.3d 197, 204 (1st Cir. 2004), vacated, 418 F.3d 67 (1st Cir. 2005).  \\
\textsuperscript{272} Councilman, 418 F.3d 67.  \\
\textsuperscript{273} Id.
\end{flushright}