WORKPLACE PRIVACY – AN OXYMORON

By Stephen D. Lichtenstein*

INTRODUCTION

The scenario is commonplace. Jim has been working hard as have all his colleagues. Recent tragic world events and the bleak outlook for the economy and e-commerce, in general, have negatively affected them. In an effort to *cheer up* the workplace environment, Jim turns to his workplace computer and surfs the Net for joke sites. He accesses *tastelesstuff.com* and copies several jokes all of which are either critical of managers and executives or are racially or sexually insensitive. He emails them to his colleagues one of whom complains to human resources. His employer receives an email of the jokes and sends Jim a termination notice. [1]

Like many companies, Jim's company should have a policy regarding employer monitoring of employee's computer use and email.[2] Under what circumstances will the courts uphold the termination? Can Jim successfully argue that he enjoyed a reasonable expectation of privacy in the workplace?[3] Seemingly, some form of judicial process would ensue. It is to be noted that this area of the law is not yet settled and probably will not be in the immediate future.[4]

---

*Professor of Law, Chair – Law Department, Bentley College, Waltham., MA

[1] See 1999 Workplace Email Abuse Study, Elron Software Corp. (http://www.elronsoftware.com/pdf/1999_Email_study.pdf), where it was determined that over 85% of the respondent employees indicated that they use employer email for personal use, over 60% visit sexually explicit Web sites and more than half received inappropriate workplace emails.

[2] See 2000 Workplace Privacy Survey, Society for Human Resource Management and West Group, where 72% of the 722 human resource respondents reported that their companies/organizations had a formal written policy on monitoring Internet use and 70% had the same regarding email. 94% reported that the policies were formally shared with employees. Almost all the respondents indicated that monitoring was usually conducted only for cause. See also The Extent of Systematic Monitoring of Employee Email and Internet Use, Privacy Foundation, July 9, 200; Nielsen//NetRatings; U.S. Bureau of Labor Statistics; International Labour Organization. Their findings revealed that out of a total U.S. workforce of 140 million, 40 million work online 14 million (35%) of which are routinely monitored. Globally, out of a total workforce of 3 billion, 100 million work online 27 million (27%) of which are likewise monitored.

[3] If this hypothetical had occurred in France, an employee's workplace privacy would enjoy more protection than in the U.S. See *Nikon France v. Onos*, Cass. Soc., Arrêt No. 41-64, October 2, 2001 where Onos was fired by Nikon after one of its managers discovered he was using his workplace computer for personal activities. The court ruled in favor of Onos holding that an employee enjoyed a right to privacy *even during and at his place of work*, a right that extended to *secret correspondence*. The court did not specifically deny the employer the right to prohibit employee personal use of its computers. However, it placed limits on an employer's right to do so particularly if the employer's reason were to discover if the employee were engaged in a wrongful act.

[4] Consider *Curtis v. DiMaio*, 46 F. Supp. 2d 206 (E.D. N.Y. 1999). *aff'd*, 205 F.3d 1322 (2d Cir. 2000). Brenda Curtis and other plaintiffs, former at-will employees of Citibank, brought this action alleging that they were forced to work in a racially hostile environment. Plaintiffs allege that Defendants used Citibank's email system to send emails that contained two jokes that were racially and ethnically offensive to African-

However, as this paper shall ultimately conclude, in cases such as that described above, reasonable business judgment dictates the creation and implementation of a workplace computer usage monitoring policy applicable to email, surfing and chat room activities. A recent article in the New York Times[5] presents facts employers should closely scrutinize and take into consideration if they are contemplating whether or not such policies are necessary and should therefore be adopted. The article pointed out that due to the alarming increase in the number of claims for workplace discrimination and harassment, insurance companies covering such claims have doubled and, in some instances, tripled their rates for such coverage while others have simply discontinued theirs. Thus, it is to be reiterated that it is legally and ethically prudent for the employer to fashion a written workplace privacy policy that includes monitoring of computer use while at the same time providing adequate safeguards and protections for employee privacy rights so as to survive judicial scrutiny.

In the hypothetical under discussion, Jim's employer would no doubt argue it owned the workplace computer and that implicit with that possessory interest was the right and obligation to insure its proper and most cost effective use. The attorney and accountant for the employer would not underestimate the obligation owed by the business to its stakeholders to take whatever steps necessary. These would include a computer monitoring policy the purpose of which would be to reduce the potential for legal liability that could arise out of the actions of the employees for electronic communications that could be found to be in violation of the laws related to workplace discrimination, harassment, and obscenity as well as those involving intellectual and trade secret property rights. Without an effectively drawn and implemented workplace monitoring policy, and in the presence of allegations of violations as described above, expensive litigation is likely to ensue. Accordingly, an employer would be well advised to consider *Nardinelli et al v. Chevron.*[6]

In *Nardinelli*, the Defendant had an anti-harassment policy that mandated awareness training for all employees. However, it had no monitoring policy. The Plaintiffs alleged sexual harassment arising out of emails sent by other employees that discussed *25 reasons why beer was better than women*. Rather than engage in litigation, Chevron settled out of court for 2.2 million dollars. With a workplace monitoring policy in place, a different less costly disposition could have resulted. Consider a more recent decision, *Blakey v. Continental Airlines.*[7]. In 1989, Blakey became Continental's first female pilot with most of her flights originating from the Newark Airport. In 1991, she complained to her superiors about receiving pornographic pictures in her cockpit along with being subjected to vulgar comments. Neither abated and in 1993 she filed a claim under Title VII of the Civil Rights Act of 1964 with the EEOC for sex discrimination and retaliation

---

Americans. The Defendants conceded that the jokes were insensitive. The court concluded that notwithstanding the fact that Plaintiffs qualified as members of a protected class under Title VII of the Civil Rights Act of 1965, they could not establish that two jokes created a hostile work environment where severe or pervasive harassment existed.

[5] *Surge in Bias Cases Punishes Insurers and Premiums Rise*, Reed Abelson, January 9, 2002 P. 36.

[6] No. 945302, Superior Court, California (1995).

[7] 751 A. 2d 538 (N.J. 2000).

for her complaints. While the case was pending in a New Jersey trial court, the harassment continued now in the form of derogatory postings on the company online bulletin board (outside the workplace). One of the comments referred to her as a *feminazi* and also questioned her ability as a pilot. The trial court dismissed the suit but the New Jersey Supreme Court reversed the trial court and awarded Blakey 1.7 million dollars in damages. The Court held that although the employer's online bulletin board might not have a physical presence in the workplace, it would be considered closely related to the workplace environment so that harassment posted on it, as in the present case, would be regarded as happening in the workplace.[8] The Court further reasoned that here the employer had notice of the co-workers harassment activities and, therefore, with that knowledge came the legal obligation and duty to remedy them or be subjected to a claim of a hostile work environment rife with sexual harassment.[9] The Court reached this conclusion notwithstanding the fact that the bulletin board was outside the workplace.[10]

Where employers take prompt and decisive remedial action concerning employee wrongdoing such as in the above cases, the courts are likely to take a position favorable to the employer.[11] Although the cases discussed herein thus far point to a monitoring policy, it is appropriate and relevant to also discuss the privacy laws governing the hypothetical presented above with the end result perhaps providing additional guidance as to under what circumstances an employer has a right to monitor such usage without infringing upon the employee's right to privacy. Attention is to be focused on the common law of torts, state and federal constitutional law and statutory law.

SOURCES OF THE RIGHT TO PRIVACY

U.S. and State Constitutions

The U.S. Supreme Court has interpreted four[12] of the first ten Amendments to the Constitution, as well as the Fourteenth, as providing at least a penumbral or implied right (not an enumerated or express right) to privacy providing protection only against

---

[8] Id. p.541.
[9] Id.
[10] Id. Here the Court reasoned that if the employer took no steps to correct the harassment outside the workplace, other employees might take this as a signal that such conduct would go unpunished by the employer.
[11] See *Schweinn v. Anheiser-Busch, Inc*., 1998 WL 166845 (N.D. N.Y. 1998) where the court dismissed a sexual harassment suit against an the employer because it took prompt action to stop it that included warnings to the employees sending he harassing emails. See also, *Daniels v. WorldCom Corp*., 1998 U.S. Dist. LEXIS 2335 (N.D. Texas 1998), Daniels and others allege in this action that they were discriminated against by racially harassing emails (4 racial jokes) sent by employees. The Human Resources Manager issued a strong verbal warning to the sender of the jokes and placed a written reprimand in her file. Later she was dismissed and the remaining employees charged with also sending the emails were warned against continuing their actions. The court granted the employer's Motion for Summary Judgment holding that under Title VII, claims for harassment and retaliation must first be brought to the EEOC and not the district court and that the employer was not guilty of negligence since the employer acted reasonably and speedily in remedying the situation once it came to its attention.
[12] First, Fourth, Fifth and Ninth Amendments.

government intrusions[13] and no express right to privacy. Similarly, many state constitutions imply a right to privacy similar to that of the U.S. Constitution while others enumerate it.[14] It should be noted that to date the courts, both state and federal, have reached no consensus as to the circumstances under which a right to workplace privacy should or should not be recognized. However, the cases and statutory interpretations do provide guidance in pursuing causes of action for invasion of privacy.

Common Law of Torts

The common law might provide a viable legal basis for establishing a right to privacy. The right began to surface when Judge Thomas Cooley stated that individuals had *a right to be let alone,*[15] a right that inured to society and one that was to be protected from unwarranted intrusions or interferences. Louis Brandeis and Samuel Warren also argued for recognition and acceptance of this right.[16]

---

[13] In *O'Connor v. Ortega*, 480 U.S. 709 (1987), officials at a California hospital suspected Dr. Ortega of management improprieties, sexual harassment and removal of a hospital computer. Without a warrant, they searched his office and seized evidence from his file cabinets and used it against him in a disciplinary proceeding before the California State Personnel Board leading to his discharge. The issue before the Court was whether the search violated Ortega's reasonable expectation of privacy protected by the Fourth Amendment. The Court held that what was reasonable depended on the context within which the search occurred and required balancing the employee's legitimate expectation of privacy against the government's need for supervision, control and efficient operation of the workplace. The Court also reasoned that to require a warrant every time an employer wished to enter an employee's office, desk or file cabinet for a work-related purpose would seriously disrupt the routine conduct of business and would be unreasonable. Further, the Court stated that the standard of reasonableness must be decided on a case-by-case basis. Toward that end, the case was remanded to determine on the facts the reasonableness of the search and whether it was justified. More recently, in *Albert Muick v. Glenayre Electronics*, No. 98 C 3187 (7th Cir. February 22, 2202) the plaintiff had been issued a company laptop and the defendant had in place a computer usage policy allowing it to inspect employee computers. A federal law enforcement agency suspected the plaintiff of having evidence of child pornography on his laptop. Upon receiving a search warrant from the law enforcement officials, defendant turned the laptop over to them. Subsequently, the plaintiff was convicted of receiving and possessing child pornography based on the evidence found on his laptop. He claimed 4th and 5th Amendment violations of his rights. The court disagrees and upholds the district court's dismissal of these claims on two grounds. First, as a private corporation, the defendant could not be liable for violating federal rights. The court also reasoned that the defendant only turned over the laptop after being served with a search warrant. Second, and probably more significant for our discussion, because of the policy in place, the plaintiff could not establish one of the prerequisites for a successful claim under the 4th Amendment namely that he enjoyed a reasonable expectation of privacy. Similarly, see *USA v. Eric Neal Angevine*, No. 01 – 6097 (10th Cir. February 22, 2002) where Oklahoma University (a government/public employer) had a similar policy as in the above case and appropriated one of its professor's computers who was suspected of possessing child pornography on his computer. The court held he enjoyed no reasonable expectation of privacy and therefore no Constitutional right to privacy. Further, the court held that under Oklahoma law, all email was considered a public record not entitled to a right to privacy or confidentiality except where otherwise provided either under Oklahoma of federal law.

[14] See for example, California Constitution, Article I, Sec. I, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness and privacy."
See also Florida Constitution, Article I, Sec 23, "Every natural person has the right to be let alone and free from governmental intrusion into his private life…" See also, *Shoars v. Epson*, Cal. App. No. B0773234 (April 14, 1994).

[15] A Treatise on the Law of Torts, Judge Thomas Cooley, 1880.

[16] Louis Brandeis, Samuel Warren, *The Right to Privacy*, Harvard Law Review, 1890.

DeMay v. Roberts[17] was one of the first cases in which a plaintiff successfully claimed a right to privacy. In that case, the plaintiff went into child labor and her physician, the defendant, Roberts, was called to her house for the delivery. It was a stormy night so Roberts invited a young man to carry a lantern and to assist him. Without the plaintiff's permission, the young man witnessed the childbirth. Roberts was slapped with a lawsuit in which the court held that the plaintiff had a common law right to privacy in the birth of her child and was entitled to damages against the defendant for violating that right.[18]

With the beginning of the Twentieth Century, the right to privacy began to slowly evolve.[19]

The Restatement of Tort (2nd)[20] describes four common law intentional torts for the invasion of privacy that would probably be the best genesis for establishing a right to privacy in a suit by an employee against his employer for accessing email or computer usage. They include *Intrusion upon Seclusion*,[21] *Public Disclosure of Private Facts Causing Injury to Reputation*,[22] *Publicity Placing Another in a False Light*,[23] and *Misappropriation of a Person's Name or Likeness Causing Injury to Reputation*.[24] The

---

[17] 46 Mich. 160, 9 N.W. 146 (1881).
[18] Id.
[19] *Pavesich V. New England Life Insurance Company*, 50 S.E, 68 (1905) where the Georgia Supreme Court held that the Defendant violated the privacy rights of the Plaintiff when it published his picture without his permission in an ad.
[20] Sections 652B-E.
[21] Section 652B, *Intentionally intruding, physically or otherwise, upon the solitude or seclusion of another in his private affairs or concerns.*
[22] Section 652C, *Publicly disclosing or transmitting highly private or personal information about another that causes damage to their reputation*.
[23] Section 652 D, *Falsely connecting a person to an immoral, illegal or embarrassing situation causing damage to their reputation*.
[24] Section 652 E, *Using the name or likeness of a living person without their permission resulting in damage to their reputation*. See *Howard Stern v. Delphi Services Corporation*, 165 Misc. 2d 21, 626 N.Y.S. 2d 694 (N.Y. Sup. Ct. 1995), where the Plaintiff, the famous radio shock-jock, Howard Stern, ran for Governor of N.Y. as a publicity stunt. Without permission, the Defendant, an online news provider, ran a picture on its online news bulletin board of the Plaintiff with his buttocks exposed. The Defendant claimed it did so to promote its news related products. The Plaintiff sued for invasion of privacy alleging that since the Defendant published the picture without permission, it resulted in a misappropriation of the Plaintiff's name and likeness thereby causing him injury. The court disagreed and held that since the Stern was a public figure, his candidacy was newsworthy and the Defendant had a right to publish Stern's name along with the picture in order to advertise or promote its news related products. The Defendant's actions were entitled to First Amendment protection and the Plaintiff's right to privacy was not invaded since he had no reasonable expectation of privacy. For a more recent case, see Felsher v. University of Evansville, Ind. Sup. Ct., No. 82S04-0008-CV-477 (October 1, 2001). Here, Felsher, a French professor at the University of Evansville was fired in 1991 and six years later set up Web sites and email addresses that included parts of the names of three university officials as well as the letters *UE*. He posted articles in which he alleges the three were guilty of wrongdoings. He then sent emails to other Universities in which he nominated them for certain teaching positions, and directed those interested to visit his Web sites where they could read the articles and their allegations that he posted. The three and the university bring claiming invasion of privacy. The Court found Felsher guilty of misappropriation of the official's names and enjoined him from using the three names along with the letters *UE*. The injunction did not prohibit future nominations Felsher might send in his own name. As far as the university's claim, the Court ruled that

elements of proof required for each of these torts are generally similar.[25] It should be noted this is still an unsettled area of the law with state and federal courts as well as existing legislation providing no consensus as to the law.

Notwithstanding the fact that this whole area of privacy rights regarding the workplace is still unsettled, perhaps some of the more significant cases illustrative of these torts may serve to provide some semblance of predictability if an employee were to pursue a cause of action for the tortious invasion of privacy.

Smyth v. Pillsbury,[26]*McLaren v. Microsoft Corp*[27] and *Bourke et al. v. Nissan Motor Corporation*[28] are three of the more significant and relevant cases applicable to tortuous invasion of privacy. Both involve actions for *Intrusion Upon Seclusion*, probably the tort most likely to succeed in providing protection for employer workplace invasions of privacy. In *Smyth*, the Defendant informed its employees that their email was confidential and would not be used as a basis for termination of their employment. Smyth received two emails from his supervisor at home over his employer's computer. Both were directed at management with one stating; *kill the backstabbing bastards* while the other describes the company picnic as the *Jim Jones Kool-aid Affair*. Relying on the employer's assurances, Smyth responded by sending similar emails. The emails were intercepted and Smyth was fired. The court held that Smyth enjoyed no privacy right under the common law tort for *intrusion upon seclusion* or under federal legislation.[29] It reasoned that there existed no reasonable expectation of privacy in inappropriate and unprofessional comments despite assurances that an employer would keep them confidential. Further, the court decided that the invasion was not substantial enough given the circumstances nor would it be considered offensive to a reasonable person.[30]

In *McLaren*, the Plaintiff, Bill McLaren, was employed by Microsoft and, in 1996, was suspended pending an investigation into accusations of sexual harassment and other improprieties. Subsequently, he was fired. As his sole cause of action, McLaren alleged that Microsoft had invaded his privacy (intrusion upon seclusion) by "breaking into" and accessing emails stored in his personal folders maintained by him on his office computer and releasing them to third parties. According to McLaren, these personal folders were restricted by a personal password created by and known only to him. Although he conceded that Microsoft could decrypt his personal password, that in allowing him to

---

under the Restatement (Second) of Torts, the privacy tort of misappropriation applied only to natural persons and not corporations (artificial legal beings). Accordingly, the Court advised that the rights of the University might best be enforced in federal trademark and other state laws. See *Warner-Lambert Co. v. Execuquest Corp*. 691 N.E. 2d 545 (Mass. 1998) which held that since a corporation was not an *individual* with traits of a *highly personal or intimate nature*, Mass. privacy law did not provide protection to corporations.

[25] Intent or knowledge (*scienter*) on the part of the defendant, plaintiff must establish he had a reasonable expectation of privacy, the disclosure must be highly offensive to a reasonable person, and there must be communication or publication to a significant segment of the community.

[26] 914 F. Supp. 97(E.D. Pa. 1996).

[27] Case No. 05-97-00824, 1999 Tex. App. Lexis 4103 (Tex. Ct. of App., May 28, 1999).

[28] No. B068705, 2nd App. Dist. Cal., July 26, 1993.

[29] Electronic Communications Privacy Act of 1986 (see discussion later).

[30] 914 F. Supp 97, see *supra* at 101.

have a password for his personal folders, a reasonable expectation of privacy was created by Microsoft that his folders would be free from intrusion and interference. McLaren characterized Microsoft's actions as an intentional unjustified and unlawful invasion of privacy under Texas law.[31] The court concluded that McLaren enjoyed no reasonable expectation of privacy because the emails stored in his personal folders first traveled through various points in Microsoft's email system before arriving in McLaren's folder[32]. Thus, it was accessible by Microsoft before it reached the folder. Similar to the reasoning in *Smyth*, the court also decided that a reasonable person would not consider Microsoft's actions to be highly offensive because the folders were not intended to be a depository for personal items but rather for performing job related functions. Further, the court concluded that the emails stored in the folders were not McLaren's personal property but merely an inherent part of the office environment and, in any event, Microsoft's interest in preventing inappropriate and unprofessional comments, or potentially illegal activities such as sexual harassment, outweighed McLaren's claimed privacy interest.[33]

In *Bourke, et al. V. Nissan Motor Corporation*, Bourke and the others in her work group were employed as computer systems specialists, essentially customer service representatives. She and the others including Rhonda Hall had signed-off, acknowledging Nissan's computer usage policy that expressly limited computer usage to business-related purposes. It was also known by its employees that Nissan would randomly check employee email to insure compliance with the policy. One of Bourke's co-workers, Lori Eaton, was conducting a training session to demonstrate the uses of email as an aid to management. She randomly accessed one of Bourke's emails that contained information of a personal, sexual nature that was not business-related. Eaton told her supervisor who issued written warnings to Bourke (and others) for violating the company policy. This resulted in Bourke receiving low job performance ratings after which she subsequently resigned. Rhonda Hall was fired. Bourke, Hall and the others sued alleging *intrusion upon seclusion*, violation of their constitutional right to privacy, violation of wiretapping statutes, and, in Hall's case, wrongful discharge in violation of public policy that is, retaliatory firing for filing complaints with Nissan's human resources department for Nissan's invasions of privacy precipitated by their accessing and reading the emails. The court of appeals affirmed the trial court's grant of summary judgment for Nissan. The court believed the constitutional right to privacy under California law was broader than the common law tort for *intrusion upon seclusion*. Accordingly, it restricted its discussion to the constitutional claim reasoning that since the plaintiffs knew of the policy and the random accessing, they enjoyed no reasonable expectation of privacy. This fact would have also yielded the same result had the court focused on the *intrusion upon seclusion* claim. Further, there was no evidence of wiretapping by Nissan nor was there a wrongful discharge in violation of public policy since Nissan's actions resulted in no constitutional violations.

---

[31] *McLaren*, see *supra* at 4106.
[32] Id. at 4107.
[33] Id.

These cases should be contrasted with the opposite decision reached in *Restuccia v. Burk Technology,*[34] a trial case decided under a Massachusetts's law[35] that provides protection for privacy rights against *unreasonable, substantial or serious interference*.[36] In *Restuccia*, the employer suspected employees had been sending personal emails over the employer's email system in which the employees referred to him by various nicknames and also chatted about an alleged extramarital affair the employer was having with another employee.[37] The employer allowed employees to use the system for personal messages, to access the system with personal passwords, and had never told the employees that the employer could access their email. Without offering reasoning, the court denied the employer's motion for summary judgment and decided that, based on the evidence and workplace environment created by the employer, there existed an issue of fact as to whether the employees enjoyed a reasonable expectation of privacy to be protected under law.[38]

FEDERAL LEGISLATION – THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (1986)

Jim's privacy rights under federal legislation would best be discussed by focusing on the Electronic Communications Privacy Act of 1986 (ECPA).[39] Congress passed the Act and its two major Titles because of the increasing privacy concerns precipitated by the growth in the use of computers. The ECPA amended existing federal anti-wiretapping statutes[40] so as to extend privacy protection to radio pagers, cell phones, private communication carriers, and electronic communications such as email.

Title I of the ECPA[41] provides that any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept, endeavor to intercept any wire, oral, or electronic communication shall be punished or subject to suit.[42] Title II[43] addresses stored communications and provides that whoever intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to an electronic communication while it is in electronic storage in such system shall be punished.[44] Further, a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person

---

[34] 5 Mass. L. Rptr, No. 31, 712 (Middlesex Superior Court, 1996).
[35] Mass. General Laws Chapter 214 δ1B - provides a cause of action in tort for violations of invasion of privacy.
[36] Id.
[37] 5 Mass. L. Rptr, No. 31, 713.
[38] Id. at 714.
[39] 18 U.S.C. δ2510-2520 – Interception of Electronic Communications.
[40] Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Note, this Act only afforded protection to wire and oral communications.
[41] 18 U.S.C. δ2511.
[42] 18 U.S.C. δ2511 (1) (a). (This section of the Act provides for both civil and criminal sanctions).
[43] 18 U.S.C. δ2701 – Stored Electronic Communications.
[44] 18 U.S.C. δ2701 (a).

or entity the contents of a communication while in electronic storage by that service.[45] Two important cases illustrate the application of the ECPA. In *Andersen Consulting v. UOP,*[46] the defendant licensed process technologies and supplied catalysts, specialty chemicals and related products to the petroleum and gas processing industries. It hired the plaintiff to perform a systems integration project during which the plaintiffs had access to and used UOP's internal email system to communicate with each other.[47] The defendant became dissatisfied with the plaintiff's performance and terminated the project hiring replacements. The defendant brought suit in a Connecticut state court against the plaintiff claiming breach of contract, negligence and fraud.[48] The plaintiff countersued for defamation.[49] While these suits were pending, the defendant accessed and disclosed the contents of the plaintiff's messages stored on the defendant's email system to the Wall Street Journal which published an article entitled, *Email Trail Could Haunt Consultant in Court.*[50] The plaintiff claimed a violation of his rights under the ECPA.[51] In establishing his claim, the plaintiff had to prove that the defendant was providing an electronic communication service to the public. It failed to do so and the court ruled in favor of the defendant holding that under the facts of the case, since the defendant's email system was internal, it was not providing an electronic communication system to the public as required by the ECPA. Accordingly, the court granted the defendant's motion to dismiss the plaintiff's claims.[52] The other illustrative case is *Robert Konop v. Hawaiian Airlines.*[53] In this case, the plaintiff was a pilot for the defendant airline. During union negotiations with the Airline Pilots Association (ALPA), the plaintiff became upset and created a web site where he posted messages critical of the defendant's president and urged employees to seek another union to represent them. The site was only accessible by receiving a user name and password assigned by the plaintiff. Once received, they were not to be disclosed to others. The defendant attempted but failed to access the site but successfully enlisted the aid of another pilot who gave his user password to the defendant's vice-president. He pretended to be a pilot, logged on and accessed the site. The contents of the messages were disclosed to the defendant's president and the ALPA. Both indicated their disapproval to the plaintiff. The plaintiff brought suit alleging both Title I and II ECPA violations. He also alleged a violation of the Railway Labor Act arising out of the defendant's unauthorized surveillance of union organizing activities. The court agreed with the plaintiff holding that under Title I,[54] plaintiff's messages were electronic communications within the meaning of the ECPA and as such were intercepted even if the interception occurred, as it did here, after the communication was posted on the web site.[55] Further, it held that under Title II[56] the contents of the plaintiff's messages

---

[45] 18 U.S.C. d2702 (a)(1).
[46] 991 F. Supp. 1041 (N.D. Ill 1998).
[47] Id. at 1042.
[48] Id.
[49] Id.
[50] June 19, 1997
[51] 991 F. Supp. 1042
[52] Id.
[53] 236 F. 3d 1035 (9th Cir. 2001).
[54] 18 U.S.C. d 2510 et seq.
[55] *Konop*, supra at 1047.
[56] 18 U.S.C. d 2701 et seq.

were posted on a secure site and constituted electronic communications in storage to be protected from unauthorized access.[57] Essentially, *Konop* establishes that an electronic communication can be intercepted while in storage regardless if the intended recipient has yet to receive it. This interpretation of the ECPA is at odds with decisions rendered by other courts.[58]

Exceptions Under the ECPA

Under Title I and Title II of the ECPA there are two similar exceptions[59] with one additional exception provided under Title II that warrants discussion. The first exception is the Prior Consent Exception[60] where the employee gives consent to the employer to monitor his computer usually pursuant to an expressed computer usage and monitoring policy. As will be suggested later, the policy should be written. In any event, the extent of the consent is not limitless.[61] Additionally, there is precedent holding that once an employer determines that the employee is transmitting personal messages, the monitoring must stop.[62]

The second exception is the Business Extension or Ordinary Course of Business Exception[63]. Here an employer can intercept an employee's email if it uses an allowable ECPA device[64] furnished by a provider of wire or electronic communication service in the ordinary course of its business. The interception will be upheld if the employer was doing so to protect its business interests.[65] The problem with using this exception for

---

[57] *Konop*, supra at 1048.

[58] See *Eagle Investment Systems Corp. v. Tamm*, D. Mass., No. 01-10192-JLT, May 22, 2001 where an email was intercepted by the defendant after it was sent to the plaintiff by one of its employees and not *during transmission* as required by the ECPA. Thus, it was in storage when it was intercepted. Noting that the Circuits have split in their interpretation of this requirement, the court ruled that it would not rule as the 9th Circuit did in *Konop*, but rather would adopt the 5th Circuit view that the interception had to occur *during transmission* reasoning that if it so intended, Congress would have indicated that interception could occur after the communication was in storage.

[59] 18 U.S.C. d 2511 (Title I), 18 U. S. C. d 2702

[60] 18 U.S.C. d 2511 (2) (d) (interception under Title I) and d 2702 (b) (3) (accession under Title II).

[61] *Sanders v. Bosch*, 38 F. 3d 736 (1994) where an employer, who with prior consent to monitor, continuously (24/7) monitored an employee it suspected of wrongdoing, the court held the monitoring to be excessive.

[62] See, Watkins v. L.M. Berry & Co., 704 F. 2d 577 (11th Cir. 1983), where the employer had a monitoring policy applicable only to business calls and intercepted a personal call made between the plaintiff and a friend, the court held it to be a violation of the Federal Wiretap Act since the employee only consented to the monitoring of business calls.

[63] 18 U.S.C.d 2702 (b) (2)

[64] 18 U.S.C. d 2510 (4).

[65] See *Deals v. Spears*, 980 F. 2d 1153 (1992). The defendant suspected the plaintiff of burglarizing his store and records all plaintiff's phone calls made on store phones. He gave no notice and received no permission to do so. The defendant told the plaintiff to cut down on personal calls or he might be monitored. A month and a half later, the defendant finds out that the plaintiff is not a burglar but has been

Jim's case, and in general, is that it has yet to be applied to email in that it has yet to be decided if an employer's computer network and equipment satisfy the ECPA's definition of an electronic device capable of completing an interception. The Act refers to an electronic, mechanical or other device such as telephone or telegraph equipment that can be used to intercept a wire, oral, or electronic communication.[66] It does not mention a computer as being such a device. It will be up to the courts to decide if an employer's main computer will qualify as such a device under this exception.

The third exception is the System Provider (aka Online Service Provider) Exception.[67] This exception provides that an employer shall not be liable where it maintains and provides the email system and an interception, disclosure or use of the email is a necessary incident to the rendition of their service or to the protection of the rights or property of the provider of that service. This exception appears to protect a private employer from liability under the ECPA for monitoring employee emails transmitted through its internal (company) email system. To date, there has been little case law under this exception. In *Bohach v. City of Reno*,[68] a police department that provided its employees with an internal email system did not violate Title II of the ECPA when it accessed the email messages of two of its police officers who were allegedly involved in illegal activities.

It is apparent that Congress' intent in including this exception was that employer provided email systems were to be excluded and the right to monitor employee email, although not absolute, would pass judicial scrutiny. Thus, as far as Jim is concerned, he most likely will not find success under the ECPA.

A SUGGESTED COURSE OF ACTION AND THE NEED FOR A POLICY

By now it should be obvious that an employee enjoys only a modicum, if any, expectation of privacy in the workplace. A recent case[69] extends that modicum to the use

---

selling goods at cost to his friends. He is fired and sues under the ECPA. The court held that although the employer had a right to monitor for unauthorized use of its phones, the scope here was excessive, intrusive and beyond what was necessary to protect its business interest.

[66] 18 U.S.C. d 2510 (4).

[67] 18 U.S.C. d 2702 (5).

[68] 932 F. Supp. 1232 (1996). See also, *Flanagan v. Epson America*, No. BC007036 (Cal. Super. Ct., January 4, 1991), where Epson provided a company email system, the court ruled the System Provider exception applied to the employer when it monitored the email of several hundred of its employees without their consent.

[69] *Robert Zieminski v. TBG Insurance Services, Inc*., No. B153400 (Cal. Super. Ct., February 22, 2002). The defendant provided the plaintiff with a computer for work at home. He had signed-off on the company's electronic and telephone equipment usage policy as well as agreeing in writing to allow the employer to monitor his computer use. The defendant monitors his computer and discovers the plaintiff had been visiting pornographic web sites. The plaintiff claims the sites had simply *popped up* on his computer. Nevertheless, he is fired and sued alleging that the computer was provided as a *perk* given to all senior executives so that they could work at home and also use it for personal purposes. Therefore a reasonable expectation of privacy in its use arose. The defendant contends that given the circumstances surrounding the issuance and use of the computer, it was entitled to inspect the *home* computer. The court agrees with this contention holds that even though the computer was issued for home use, it still belonged to the

of a company computer in one's virtual office (typically at home but could also include a hotel room or other out-of-workplace venue). It should also be obvious that Jim's case and the discussion above point to a dilemma for maintaining a trusting and amicable employer-employee relationship. From its perspective, the employer's goal and intent is to insure proper use of its computers thereby maximizing productivity and avoiding potential liability for misuse. The employee's perspective raises issues of distrust of one's employer that could result from monitoring as well as other surveillance activities. Here the result could negatively impact morale and productivity.

The best advice for the employer (and for Jim's benefit and protection) would be to develop and implement a written *terms of use* policy to cover computers and electronic communications. The starting point would be a consultation with the company legal counsel and other relevant parties (human resources, employees, and, if applicable, union representatives) to determine what type and scope of policy would be best suited for the company. The company culture must be given proper consideration in such discussions. The end result should be a policy that balances the employer's right to protect its interests with the employee's right to privacy.

One such suggested policy could include the following:

- Indicate the reasons for the policy.
- Apply the policy to all employees including the CEO, etc.
- Inform employees that company equipment belongs to the company and is to be used for business purposes only (some personal use might be allowed and should be specified).
- Inform employees that all messages and information stored is company property and is confidential unless made public by the company.
- Indicate zero tolerance for offensive, harassing or discriminating communications or emails.
- Prohibit employees from encrypting email without company permission.
- Establish requirements and prohibitions for employee personal web sites (do not allow company name to appear on such sites).

As far as implementation is concerned, the company should first provide an employee training program focusing on proper use of company computers and email. Additionally, the implementation should:

- Be in writing and placed in appropriate company employee manuals and literature.
- Be given to each employee who, in writing, acknowledges receipt thereof.
- Employees should be reminded yearly of the existence and content of the policy.
- Let employees know their voice mail, email, or computer files and hard drive <u>will</u> be subject to monitoring at any time and without notice (computer screen

---

employer, was subject to the policy and terms agreed to by the plaintiff, the policy was violated by the plaintiff, and his right to privacy was not violated.

warnings regarding proper use should flash on computer screens when employees first log-on and employees should be informed if the company is employing content monitoring or blocking software[70]).

- Indicate that password protection does not guarantee employee immunity from employer access.
- Indicate that violations of the Policy will lead to disciplinary action up to and including termination.
- Recognize that some personal use of the company computer is going to occur and will be tolerated (in the same sense as phone calls, visits from friends, family, etc.) but that excessive use will not be tolerated.

CONCLUSION

It is important to note that there currently exists no state or federal law requiring that employers adopt policies such as the above. In fact, many have been proposed[71] but none have yet been adopted. Also note that the above suggestions are not inclusive but rather are intended as guidelines to be used in developing a policy. There is no guarantee that having such a policy will immunize the employer from liability for claims of invasion of privacy brought by employees. However, given that most employees will follow a properly designed and implemented policy, the courts will seemingly opt to deny an employee's invasion of privacy claim absent an unjustified and complete disregard of that right by the employer.

---

[70] eSniff 1100, Pearl Software, SurfControl, SilentRunner, etc. Most of these allow for real time auditing and monitoring of computer use. MIMEsweeper and other similar software products allow the employer to block communications that contain words and phrases that could result in potential liability for the company. This would be particularly valuable if an employee disregarded the policy and transmitted offensive or harassing emails.

[71] H.R. 4908 - The Notice Of Electronic Monitoring Act (2000) sponsored by Senator Charles Schumer (D. NY), Representatives Charles Canady (R. FL) and Bob Barr (R. GA). §2711 of this Act would require employers to notify employees about email monitoring, computer and Internet use, and phone calls. The notice would have to be clear and conspicuous indicating the form of communication or computer usage that would be monitored as well as the means by which the monitoring would be accomplished. Further, the employer would have to indicate the kinds of information that would be obtained through the monitoring, the frequency of the monitoring and how the information obtained would be stored, used or disclosed.