THE MISUSE OF EMPLOYER TECHNOLOGY BY EMPLOYEES TO COMMIT CRIMINAL ACTS

Presented by

Julie A. Totten
Orrick, Herrington & Sutcliffe, LLP

ABA Section of Labor and Employment Law
Technology Committee Midyear Meeting
Miami, April 21-23, 2004

———

Julie A. Totten
Orrick, Herrington & Sutcliffe LLP
400 Capitol Mall, Suite 3000
Sacramento, CA 95814
Tel: (916) 447-9200

Fax: (916) 329-4900
email: jatotten@orrick.com

Table of Contents

Page

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

THE MISUSE OF EMPLOYER TECHNOLOGY BY EMPLOYEES TO COMMIT CRIMINAL ACTS

I. INTRODUCTION

Technology benefits the workplace by increasing productivity and efficiency. For example, e-mail is a fruit of technology that allows employees a greater sense of connectivity never felt in any previous generation. The American Management Association recently reported that, on average, a worker spends a quarter of the workday receiving, reading, and sending e-mail, with 31 percent of all respondents devoting two or more hours a day doing the same. *2003 E-Mail Rules, Policies and Practices Survey*, AMERICAN MANAGEMENT ASSOCIATION 1, 6 (2003) ("AMA Survey"). Although employees generally use technology to advance their employer's objectives, employees may also be misusing technology for illegal purposes such as downloading copyrighted materials for personal use, viewing child pornography, retaliating against an employer, and misappropriating confidential information or trade secrets, just to name a few.

Employers must take affirmative steps to combat such criminal activities. More than half of the companies in this country have engaged in some type of formal e-mail monitoring of employees. *See id.* More than nine out of 10 managers monitor their employee's use of e-mail, the Internet or other technology according to a survey conducted by Bentley College's Center for Business Ethics ("Bentley Survey"). W. Hoffman et al., *You've Got Mail . . . And the Boss Knows: A survey by the Center for Business Ethics of Companies' Email and Internet Monitoring*, 108:3 BUS. & SOC'Y REV. 285, 286, 291-92 (2003). Furthermore, 26 percent of companies in the Bentley Survey reported that they either monitor their employees' Internet and e-mail activity all of the time and 38 percent state they monitor randomly or periodically. *Id.* at 296-97. Failing to take such steps to prevent illegal acts could bring about civil liability and unwanted public exposure. Employers must not only keep pace with the advancement of technology, but also with their employees' potential misuse of technology.

II. EMPLOYEE CRIMES COMMITTED BY THE USE OF TECHNOLOGY

A. Downloading Copyrighted Materials

In a recent wave of lawsuits against individual users of peer-to-peer software (P2P networking), recording and motion picture associations declared war against those who illegally download copyrighted music. These associations have now begun to turn their attention to corporations. In fact, in April 2002, the Recording Industry Artist Association entered into a one million dollar settlement agreement with Integrated Information Systems Inc., an innovative technology and business consultancy, for allegedly allowing employees to share copyrighted digital music files on the company's server. Integrated Information Systems Press Release, *Integrated Information Systems Responds to 2001 Settlement with RIAA*, *at* http://www.iis.com/press/pressreleases2002/RIAApressrelease041202Final1.pdf (last visited March 26, 2004). Additionally, the Motion Picture Association of America and the Recording Industry Association of America have sent brochures to Fortune 1000 corporations warning against such infringement occurring on employers' networks. *See* IFPI, Copyright Use and Security Guide For Companies and Government, *available at* http://www.ifpi.org/site-

content/library/copyright-use-and-security-guide-english.pdf (last visited March 25, 2004).

Peer-to-peer software allows users to search for and download files from another user's machine wherever they may be via the Internet. *See* Lisa J. Beyer Sims, Comment, *Mutiny on the Net: Ridding P2P Pirates of their Booty*, 52 EMORY L.J. 1907, 1910 (2003). An employee need only download peer-to-peer software from the Internet onto an employer's computer to begin sharing files. With literally millions of users of peer-to-peer software, employees may conveniently (and illegally) retrieve music and other copyrighted material from other sharers.

Employees may also use their employer's bulletin board service ("BBS") to upload and download copyright materials, thereby allowing other employees access to the BBS. Once placed onto these bulletin boards, an employee may retrieve copyrighted pictures, files and data through this service. The ease of uploading and downloading copyrighted materials can be seen in *Playboy Enters. Inc.* v. *Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997). In *Playboy*, the owner of a company placed adult copyrighted pictures on his BBS, without the consent of Playboy Enterprises, and allowed users of his service access to these protected images. The owner actually encouraged his users to upload these copyrighted images to the BBS and implemented a screening procedure in which he could view all files being uploaded before placing them on the BBS. Based on these facts, the court found the owner and his company liable for copyright infringement for distributing and displaying these protected materials.

B. Child Pornography

Viewing child pornography in the workplace has become more pervasive with the advent of sophisticated networks and computers. Employees may be more prone to view child pornography in the workplace rather than at their homes, believing that authorities are less likely to track their illegal activities. Federal laws and many state laws make the mere possession of child pornography criminal. *See, e.g.*, 18 U.S.C. § 2252A(a)(5)(B) (any person who "knowingly possesses any book, magazine . . . or any other material that contains an image of child pornography" may be punished by imprisonment); CAL. PENAL CODE § 311.2.

Another federal statute incriminates a person who "knowingly uses any . . . interactive computer service . . . for carriage in interstate or foreign commerce . . . [of] any obscene, lewd, lascivious, or filthy phonograph recording, electrical transcription, or other article or thing capable of producing sound." 18 U.S.C. § 1462(b). This statute provides for broad liability because it punishes those who use the Internet or other interactive computer service to receive not only child pornography, but any obscene material. *See United States* v. *Reilly*, 2002 U.S. Dis. LEXIS 19564 (S.D.N.Y., Oct. 11, 2002). In *Reilly*, the defendant, a government employee, accessed web sites after hours that displayed nude and partially nude children engaging in sexual acts. After searching the defendant's computer and disks, federal agents found incriminating images contained therein. The defendant challenged 18 U.S.C. section 1462 claiming that he had a constitutional right to download and review these materials. The court rejected this argument and explained that while a person may have a constitutional right to *possess* obscene materials, Congress may prohibit the *method of receiving* obscene materials – the Internet – which does not violate the constitution.

C. Employee Sabotage

With a greater reliance of connectivity, employers must deal with the real threat of employee sabotage of its computer system. Disgruntled employees are employing this sophisticated and illegal technique to retaliate against unsuspecting employers. In one of the worst cases of computer sabotage, Timothy Lloyd activated a software-bomb in his employer's software system that resulted in the permanent deletion of over 1,200 computer programs. *See United States* v. *Lloyd*, 269 F.3d 228 (3d Cir. 2001). His employer, Omega Engineering Corporation, manufactured high-tech instruments for NASA and the Navy. Lloyd worked for Omega as its only computer system administrator. After receiving counseling on several occasions about his abusive behavior, Omega terminated Lloyd. Not long after, Omega discovered the mass deletion and purging of critical programs and files from its computer system. The sabotage led to the company foregoing millions of dollars in sales and contracts with the government. Lloyd eventually was convicted of computer sabotage under several federal statutes.

D. Misappropriation of Confidential Information

Employees may also seek to gain unauthorized access to their employer's computer system to obtain proprietary or trade secret information. Two former Cisco accountants gained unauthorized access to Cisco's computer system to distribute to themselves Cisco stock worth approximately $4 million. *See United States* v. *Osowski*, No. Cr. 01-20055 (N.D. Cal. April 4, 2001). While reconciling a discrepancy in outstanding stock shares, Osowski realized that he could request a payout of shares by using the same control number twice. After consulting with his manager, Wilson Tang, they decided to use this knowledge to request stock to be transferred into their Merrill Lynch account. Tang and Osowski then liquidated much of the stock by buying a Mercedes, a diamond ring, and a Rolex watch. Becoming suspicious, Cisco informed authorities about the unusual activity after receiving a tip from Merrill Lynch. Had it not been for the tip, the employees may have likely been able to get away with the company's oversight.

In *U.S. GreenFiber* v. *Brooks*, No. 02-2215 (W.D. La. Oct. 25, 2002), an employer sued Brooks, a work-at-home employee, for destruction of business-related documents and violation of state trade secret protection law. Brooks worked as a quality control manager from her home using a company-owned computer. Following her termination, Brooks refused to return the computer that contained sensitive company documents and information. Instead, Brooks held the computer hostage, threatening that she would turn over the business-related materials to her employer's competitors. Before agreeing to return the computer, Brooks deleted all documents, e-mails and application programs. She was aware of the company's policy of protecting confidential information and trade secrets. The court granted the employer compensatory damages for Brooks' violation of federal and state laws.

In another misappropriation of trade secret case, *People* v. *Hawkins*, 98 Cal. App. 4th 11 (2002), Hawkins was convicted of a felony for knowingly accessing and taking data from a computer system. Hawkins worked for his employer, Network Translation Incorporated ("NTI") (which was later bought by Cisco Systems Incorporated), as a sales engineer and technical support person. While at NTI, Hawkins had access to source code and inside information, including access to NTI's Private Internet Exchange and firewall software. After leaving Cisco,

he began marketing a software similar to that of NTI's Private Internet Exchange software. Cisco eventually discovered Hawkins' plan to market his software and informed authorities of the possible misappropriation. Relying on California Penal Code section 502, which makes it a criminal offense to knowingly access a computer system or network without permission, the court affirmed Hawkin's conviction.

Employees may also illegally disclose a company's intellectual property and confidential information to its competitor for gain or retaliation against an employer. In *Near North Nat'l Group* v. *Cheley*, No. 02C4489 (N.D. Ill. June 19, 2002), three employees who were terminated, allegedly accessed confidential information and e-mails from their employer's computer network without authorization. According to the complaint, these employees supplied this information to competitors, potential business partners and potential adverse litigants of their former company. In another case, *United States* v. *Stegora*, 849 F.2d 291 (8th Cir. 1988), an employee stole samples of his employer's unreleased invention of synthetic casting material for use by orthopedic surgeons. The estimated value of the research, development and manufacturing of this product was in excess of one million dollars. Seeking to use the stolen material for profit, the employee contacted his employer's competitors to offer a new and innovative product that would soon be on the market. He offered to act as their consultant for a fee of $20,000. The employee was later prosecuted under federal statues for interstate transportation of stolen property and mail fraud.

III. LEGAL CONSIDERATIONS FOR EMPLOYERS AND EMPLOYEES

A. Potential Liability For Employers

Employers must consider the potential for civil liability for allowing or failing to prevent employees from using their technology to engage in illegal activity.

1. Sexual Harassment And Discrimination

Viewing child pornography or any other sexually explicit images in the workplace may expose an employer to hostile environment sexual harassment or discrimination claims. In *Coniglio* v. *City of Berwyn*, 1999 U.S. Dist. LEXIS 19426 (N.D. Ill. Dec. 15, 1999), the plaintiff's supervisor used his work computer to access pornographic sites on the Internet. Because his office was surrounded by glass walls, employees, including the plaintiff, frequently viewed graphic images unwillingly. Plaintiff also began receiving unsolicited e-mails from pornographic Internet sites. The district court refused to deny defendant's motion to dismiss the plaintiff's suit for sexual harassment and intentional infliction of emotional distress because it found that the plaintiff could show that the supervisor harassed her and subjected her to emotional distress.

Additionally, employers should monitor their bulletin boards and employee e-mails to ensure that no illegal or discriminatory and harassing conduct takes place. In *Blakey* v. *Continental Airlines*, 751 A.2d 538, 164 N.J. 38 (2000), the New Jersey Supreme Court reversed and remanded a case filed by a female pilot against the airlines and several individual pilots. The individual pilots allegedly posted disparaging comments about the plaintiff on a company on-line bulletin board after the plaintiff filed a lawsuit against Continental for sex discrimination. In

reversing the appellate court's dismissal of the suit, the New Jersey Supreme Court held that although the electronic bulletin board did not have a physical location within the airport terminal, it might have been so closely related to the environment of the workplace and beneficial to Continental that it should be regarded as part of the workplace. *Id.* at 549-52. The court also held that although an employer has no obligation to monitor its employees' private communications, it does have a duty "to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace." *Id.* at 552.

2. Contributory Infringement

Courts have not yet directly addressed an employer's or company's liability for the illegal downloading or sharing of copyrighted materials by its employees. However, if an employer encourages or induces an employee to engage in copyright infringement, the owner of the copyrighted material may claim contributory infringement against the employer. To prove contributory infringement, the plaintiff must show that the employer (1) with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct; (2) had knowledge of the employee's direct infringement; and (3) substantially participates by either inducing, causing, or materially contributing to that direct infringement. *See e.g.*, *Gershwin Publi'g Corp.* v. *Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971); *A&M Records, Inc.* v. *Napster, Inc.*, 239 F.3d 1004, 1019 (9th Cir. 2000) (individuals engaging in personal conduct that encourages or assists the infringement are contributory liable). While most legitimate companies would not "substantially participate" in copyright infringement, employers that know infringement is occurring on their systems and fail to deter such activity from occurring may likely be found liable. *Cf. A&M Records, Inc.*, 239 F.3d at 1021.

3. Vicarious Liability And Negligent Retention/Supervision

An injured party may also assert a claim against an employer for the acts of its employee under the theory of respondeat superior. Generally, however, the plaintiff must show that the conduct of the employee was within his or her "scope of employment." RESTATEMENT (SECOND) OF AGENCY § 228 (1958). Factors used to determine whether an employee's misconduct is within the scope of employment includes the following:

- it is of the kind he/she is employed to perform;
- it occurs substantially within the authorized time and space limits;
- it is actuated, at least in part, by a purpose to serve the employer; and
- if force is intentionally used by the employee against another, the use of force is of a kind not anticipated by the employer.

Id. Because an employee's criminal acts do not typically meet these factors, courts have found that such acts are outside an employee's scope of employment. *See, e.g.*, *Amora* v. *Metro Ford Sales & Serv., Inc.*, 206 F. Supp. 2d 947, 952 (N.D. Ill. 2002) (because employee used his

position as a car salesman to pull plaintiff's credit without permission for purely personal reasons, employer is not vicariously liable).

On another theory, employers may nevertheless be held liable for negligent retention or supervision if they hired or retained an employee with the knowledge of the employee's propensity for the sort of behavior that caused the injured party's harm. *See Haybeck* v. *Prodigy Servs. Co.*, 944 F. Supp. 326, 332 (S.D.N.Y. 1996). In *Haybeck,* the defendant, Prodigy Services Company ("Prodigy"), was sued for both vicarious liability and negligent supervision of its employee, Jacob Jacks. Prodigy is a computer service that included an on-line Prodigy chat room. Plaintiff was a customer of Prodigy and met Jacks in Prodigy's on-line chat room. Jacks spent much time chatting with the plaintiff, providing her "free time" on Prodigy's network, and allowing her to use his own Prodigy account. Jacks and the plaintiff then met in person and ultimately engaged in sexual intercourse. Later, plaintiff learned that Jacks had the AIDS virus and, after plaintiff contracted the deadly virus, she sued Prodigy for her injury.

Because the plaintiff's complaint in *Haybeck* failed to explain how Prodigy's conduct injured the plaintiff, the court characterized the complaint as alleging that Jack's failure to disclose his HIV status to plaintiff before engaging in sexual intercourse fell within the scope of employment with Prodigy (respondeat superior liability). *Id.* at 328-29. On this theory, the court sustained Prodigy's motion to dismiss because Jack's personal decision not to disclose his HIV status was not "connected" to furthering Prodigy's business nor was it "one commonly done" by an employee. *Id.* at 330-31. The court also declined to set precedent that would force employers to monitor the health of their employees.

As for Prodigy's liability for negligent hiring and retention, the court also found for Prodigy because the plaintiff failed to allege that Prodigy knew of Jack's propensity to engage in sexual intercourse without disclosing that he had AIDS. Although the *Haybeck* court sided with the employer, the plaintiff may have very well succeeded in this case (or even in another jurisdiction) if the plaintiff could have clearly articulated Prodigy's misconduct and presented evidence showing Prodigy's actual or constructive knowledge of Jack's propensity to solicit Prodigy's customers into sexual relations thereby causing harm.

B. Potential Liability For Employees

Employers that have been injured by an employee's illegal conduct (*e.g.*, misappropriation or theft of trade secrets, sabotage, etc.), may have a course for redress against the unscrupulous employee or company.

1. Computer Fraud And Abuse Act

The federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, makes it criminal to access a computer without authorization and provides civil and equitable remedies to employers. The CFAA provides companies the ability to recoup any losses suffered by the misappropriation of trade secrets and other proprietary information. While the CFAA contains many parts, two provisions of the act are highly relevant to this discussion:

- First, it is a violation to "intentionally access[ ] a protected computer without

authorization, and as a result of such conduct cause[ ] . . . a loss to one or more persons during any 1-year period . . . aggregating to at least $5,000 in value . . . ." 18 U.S.C. § 1030(a)(5)(A)(iii) and (B)(i).

- Second, it is a violation to "knowingly and with intent to defraud, access[ ] a protected computer without authorization, or exceed[ ] authorized access, and by means of such conduct further[ ] the intended fraud and obtain[ ] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." *Id.* § 1030(a)(4).

Any person who suffers damage or loss due to a violation of these provisions may bring a civil action against the violator for compensatory damages and injunctive or other equitable relief. *Id.* § 1030(g). While not explicit, a "person" under the CFAA includes natural persons and harmed corporations. *See United States* v. *Middleton*, 231 F.3d 1207, 1212-13 (9th Cir. 2000); *see also* 18 U.S.C. § 1030(e)(12). A "protected computer" is one "used in interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B). Moreover, "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." *Id.* § 1030(e)(6).

One hotly contested issue arising from the CFAA is defining what constitutes damage or loss of at least $5,000 in value. The First Circuit in *EF Cultural Travel BV* v. *Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), addressed this issue. In *Explorica*, defendants were former employees of the plaintiff, EF Cultural Travel BV ("EF"), who started a company to compete with EF. The defendants hired an Internet consultant to develop a "Scraper" to glean pricing information from EF's website. While EF's website was open to any person, the Scraper would decipher pricing information through "tour codes" found on EF's website but not understandable to the public. EF spent approximately $20,000 assessing whether its website had been compromised.

The defendants argued that the CFAA was inapplicable because EF had not suffered at least $5,000 in damage or loss from their conduct. The First Circuit disagreed. "Loss," according to the court, did not only connote monetary damages, but also a detriment or a disadvantage to EF because of the time and resources needed to determine whether the defendants breached its website without authorization. *Id.* at 585. Thus, the $20,000 expended by EF to assess whether its website had been compromised met the $5,000 threshold for loss or damage required by the CFAA. Furthermore, in *Middleton*, *supra*, 231 F.3d at 1207, the court looked at a jury instruction relating to "damage" and "loss" found in the CFAA, which was given to the jury. The court affirmed the lower court's use of this jury instruction, which allowed the jury to consider the amount of money needed to restore any data, program or system that was damaged, or resecure any data, program, system or information from further damage. *Id.* at 1213; *see also* 18 U.S.C. § 1030(e)(11). Therefore, damage or loss to an employer need not be physical damage, but could include also the resources and time expended to assess and remedy an employee's misuse of its technology.

a. The Pros And Cons of Litigation Under The CFAA

The CFAA provides an employer the right to sue when any of its provisions are violated and the jurisdictional amount (*i.e.*, at least $5000) is satisfied. However, before engaging in litigation, a company should consider both the pros and cons of filing suit against an employee or a company.

(1) Pros

- A court's equitable power may be effective in stopping an employee or a company from using misappropriated information or trade secrets.

- An employer may recoup any losses suffered by an employee's misappropriation of confidential information or trade secrets by suing the employee or company that obtained the information or trade secrets illegally.

- An employer may recoup any costs expended in determining whether an employee or a company breached its computer system or network, or the cost to repair or restructure the damaged or compromised computer system or network.

- Filing suit sends a message to other potential employees that illegal misuse of a company's computer or network will not be tolerated.

(2) Cons

- A lawsuit may be futile if an employee is insolvent and has already been convicted for the illegal conduct.

- The loss or damage has been so minimal that by filing suit the employer may risk losing on the issue of satisfying the requisite amount damage or loss required under the CFAA.

- A lawsuit may negatively affect employee morale.

- The company may be the target of negative media regarding the suit. Potential customers may be afraid of doing business with a company that has security lapses.

- The employee may file a countersuit alleging any number of theories, such as wrongful termination, discrimination, harassment and invasion of privacy.

- The expense of the litigation may outweigh the potential benefit.

IV. PRIVACY LAWS

Employers must consider an employee's privacy rights when implementing a strategy to determine if employees are using their technology to commit crimes. For instance, an employer may wish to determine whether a particular employee is using a company-owned computer to access child pornography or share copyrighted materials. An employer may thus seek to monitor an employee's Internet and e-mail activity in the workplace. The method chosen by the

employer to implement such a plan requires an understanding of an employee's privacy rights.

The Fourth Amendment to the United States Constitution protects the "rights of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." This right generally extends to protect persons from government conduct, such as police officers or federal agents, but not private employers.

The Electronic Communications Privacy Act of 1986 ("ECPA") generally prohibits interception, without a party's consent, of electronic communications "that affect interstate or foreign commerce." *See* 18 U.S.C. §§ 2510-22, 2701-11. Title I of the ECPA prohibits the actual or attempted interception, acquisition, disclosure or use of oral, wire or electronic communications. *See* 18 U.S.C. § 2511(1). The ECPA defines unlawful interception as the "acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." *Id.* § 2510(4). Title II of the ECPA prohibits unauthorized access to a wire or electronic communication while it is in electronic storage. *See* 18 U.S.C. §§ 2701(a), 2510(17) (defining electronic storage to include "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"); *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868 (9th Cir. 2002) (contents of secure website are "electronic communications" in intermediate storage).

While intercepting or monitoring an employee's e-mail or voicemail communication may very well fall under Title I or Title II of the ECPA, the statute also provides for three important exceptions:

- Under the "business extension" exception, an employer may intercept communication if done in the ordinary course of business using a qualifying device. 18 U.S.C. § 2510 (5)(a). *See also Arias* v. *Mutual Cent. Alarm Serv.*, 202 F.3d 553 (2d Cir. 2000) (recording employees' telephone conversations were within ordinary course of business for company which regularly monitored incoming and outgoing calls).

- Under the "consent" exception, an employer may monitor telephone conversations if at least one individual consents to the interception. 18 U.S.C. § 2511 (2)(d); *see also United States* v. *Mullin*, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline's monitoring of employee's use of reservation software did not violate the ECPA because the employee consented).

- The "service provider" exception permits an employer providing wire or electronic communications service (*e.g.*, e-mail or voicemail) to retrieve information maintained on that person's or entity's system in order to protect the employer's property rights. 18 U.S.C. § 2701; *see, e.g.*, *Fraser* v. *Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001) (holding that insurance company that leased computer system to agent did not violate ECPA when it retrieved stored e-mails from computer).

These exceptions provide employers with several useful alternatives in overcoming an employee's rights under the ECPA.

Employees also may claim protection of their privacy based on a common-law right to

privacy. Under common law, a person's privacy may be invaded by: (1) an unreasonable intrusion upon his or her seclusion; (2) an appropriation of his or her name or likeness; (3) public disclosure of private facts; or (4) a public portrayal of the person in a false light. RESTATEMENT (SECOND) OF TORTS § 652A (1977). Of these, intrusion upon seclusion may be the likeliest tort to be committed by an employer conducting a workplace search. Intrusion upon seclusion, according to the Restatement, is intentionally intruding "upon the solitude or seclusion of another," which is an invasion of privacy "if the intrusion would be highly offensive to a reasonable person." *Id.* at § 652B. However, demonstrating that an employer's search techniques was "highly offensive" may be difficult if an employer takes proper precautions as explained in the next section.

V. PRACTICAL TIPS FOR EMPLOYERS TO ADDRESS THE MISUSE OF TECHNOLOGY IN THE WORKPLACE

A. Practical Tips: Preventing Criminal Acts And Avoiding Liability

The following steps provide some guidance to assist in preventing the misuse of technology in the workplace and avoiding litigation.

- Employers should develop and distribute a company policy to all employees regarding the employer's electronic property and services. *See* sample policy, attached as Appendix A. Employers should also obtain the written consent of their employees to conduct searches of all company-owned equipment (including computers, e-mail, voicemail, etc.), and to monitor any Internet, e-mail or any other activity occurring on company-owned equipment.

- Employers should educate and train all employees about the seriousness of and potential ramifications for committing crimes through the use of the employer's technology.

- Employers should clearly enunciate to each employee the level of authority each employee has in accessing specific locations, documents, files or information on the employer's computer system or network.

- Employers should ensure that all business-related work is performed on a company-owned computer to allow access to the contents contained therein. Any work performed away from the office should also be done on company-owned equipment (*i.e.*, laptop).

- Employers should consider assembling an internal team of IT (Information Technology) or IS (Information Security) employees, attorneys, media relations employees and human resource professionals to deal with criminal conduct of their technology. The IT or IS employees can quickly respond to a breach or compromise of the company's network and help investigate any misconduct. Attorneys and human resource professionals should be consulted in any investigation or search of an employee's workspace (including computers, laptops, etc.) or before terminating an employee. They may also be an invaluable conduit with local authorities. Media relations employees can work with the press in dissolving negative exposure of any incidents.

- Employers should regularly monitor and search their employees' computers to determine whether they are downloading copyrighted materials, viewing or sending pornography, or engaging in any other non business-related conduct.

    - If an employer has a BBS, it should filter and review all files and information before placing them on to the system.

- Strict enforcement of the company's policy regarding downloading and uploading copyrighted materials, using Internet and e-mail, viewing pornographic images, and using any of the employer's technology may assist in preventing claims of harassment, vicarious liability and other possible claims.

- After an employee is terminated, the employer must ensure that the employee is denied access to its network or computer system. If an employee is assigned a password, the employer must ensure the password is no longer valid. An employer exposes itself to possible retaliation or sabotage if it fails to take these steps. Additionally, if an employer forgets to change the password, any subsequent access by the employee, may arguably be "authorized."

- An employer does not generally have a duty to reveal an employee's illegal use of its technology to another employer inquiring on a job reference unless the nondisclosure would result in some foreseeable physical harm. Absent this exception, the employer should, in an abundance of caution, simply state whether it would either "hire" or "not re-hire" the employee without disclosing any other information.

B. Practical Tips: Investigating Criminal Conduct

- Depending on the sophistication and seriousness of the crime, employers may choose to contact authorities immediately. Although there is no obligation to contact law enforcement authorities if an employer suspects misuse of its technology for illegal purposes, in certain situations it may be advisable to involve authorities. For instance, if an employer determines that the breach of its network was performed by an outside party utilizing highly-advanced software, or if theft of valuable information, securities or trade secrets has occurred, authorities should be contacted immediately. The following are other relevant factors that an employer may consider in determining whether to contact authorities:

    - Involving law enforcement authorities may increase the odds of catching an employee "in the act" (*e.g.*, viewing child pornography) with the knowledge and skills of these authorities;

    - Law enforcement authorities may be able to obtain wiretap, pen/trap and trace orders, and enforceable data preservation requests that are not available to private employers;

    - Working with law enforcement authorities may likely draw more public exposure, especially if they decide to prosecute the employee;

- An employer will have to coordinate its investigation and searches with law enforcement authorities, thereby giving up control over the investigation or search;

- Law enforcement authorities may be able to work with foreign countries to prosecute employees who commit crimes abroad; and

- Prosecution of employees may deter other employees from committing similar crimes.

- Employers seeking to involve law enforcement authorities should contact law enforcement authorities at the local, state, federal or international levels depending on the scope of the crime. Employers seeking to report a crime or seeking assistance relating to investigation or prosecution of a computer crime, may contact the police department within the county, state or other jurisdiction where the criminal act occurred, or contact federal authorities. The Federal Bureau of Investigation (FBI), the United States Secret Service, and the United States Customs Service have offices located in every state to which crimes may be reported. Their contact information may be located in local telephone directories. For more information about reporting computer and Internet related crimes, see http://www.cybercrime.gov/reporting.htm.

- If an employer decides to conduct an internal investigation itself, it should take the following steps to properly identify the employee who is involved in the criminal activity.

    - To prevent possible interference with an investigation, the employer should consider placing the employee under investigation on administrative or personal leave (consultation with an attorney is advised).

    - An employer should confirm with its IT and/or IS department or manager that criminal conduct occurred on a company computer or network. The IT or IS department or managers should use their resources and expertise (*e.g.*, track employee's computer activities, search contents of the employee's computer, etc.) to determine whether the employee committed any crimes or violated company policy.

    - All evidence should be confiscated and maintained by the employer. If incriminating evidence is found on a computer or laptop, for instance, the employer should immediately document and store the computer or laptop in a safe place for possible evidentiary use to defeat any potential claims asserted by the employee.

    - If the employer decides to question the employee about the alleged misconduct, it should avoid using any physical restraint or threatening the employee with arrest or termination. Employers should also avoid pressuring an employee into confessing, as this would tend to add to the threatening atmosphere.

    - Before terminating, suspending or taking any other adverse action against an employee, an employer should consult with an attorney to determine whether

sufficient evidence has been established to justify such an action.

VI. CONCLUSION

While technology is extremely beneficial, employers must remain vigilant regarding their employees' use of that technology. Ignoring the amount of access or control an employee has to an employer's computer system or network could lead to potential liability, significant monetary loss or even embarrassment. While some incidents may be completely outside an employer's control, in many instances employers could have prevented the illegal activity by taking well-calculated precautions.

APPENDIX A

Company Policy Concerning Computers, E-Mail And The Internet

The following policy governs the use of all [Company]-owned computers, e-mail, Internet access via [Company] computers and/or data lines and telephone and voice-mail systems.

Company Property

All [Company] computers, e-mail, Internet access accounts and telephone and voice-mail systems are [Company]'s property and are to be used solely for [Company] business. All software that has been installed on [Company] computers, e-mail, Internet access accounts and telephone and voice-mail systems are [Company]'s property and are to be used solely for [Company] business. Likewise, any data collected, downloaded and/or created on [Company] computers is the exclusive property of [Company] and may not be copied or transmitted to any outside party or used for any purpose not directly related to the business of [Company]. Customer information including, but not limited, to e-mail addresses, contact information, customer preferences, which is compiled by [Company], is confidential and proprietary information and should be treated as such. Unauthorized disclosure of such information at any time could be highly prejudicial to the interests of [Company] or [Company]'s customers.

Proper Use

Employees are strictly prohibited from using computers, e-mail, Internet access accounts and telephone and voice-mail systems for personal reasons or for any improper purpose. Some specific examples of prohibited uses include, but are not limited to:

- Transmitting, retrieving, downloading or storing messages or images that are offensive, derogatory, defamatory, off-color, sexual in content or otherwise inappropriate in a business environment.

- Making threatening or harassing statements to another employee, or to a vendor, customer or other outside party.

- Sending or receiving confidential or copyrighted materials without prior authorization.

- Soliciting personal business opportunities or personal advertising.

- Gambling of any kind, monitoring sports scores or playing electronic games.

- Day trading or otherwise purchasing or selling stocks, bonds or other securities or transmitting, retrieving, downloading or storing messages or images related to the purchase or sale of stocks, bonds or other securities, except as authorized by [Company].

Monitoring

Employees should expect that all information created, transmitted, downloaded, received or stored in [Company] computers, e-mail, Internet access accounts and telephone and voice-mail systems may be accessed by [Company] at any time, without prior notice. Employees should not assume that they have an expectation of privacy or confidentiality in any information transmitted or stored in a [Company] computer, e-mail, Internet access account or telephone or voice-mail system (whether or not such information is password-protected), or that deleted information is necessarily untraceable.

Employees must provide all passwords and access codes for computers, e-mail, Internet access accounts and telephone and voice-mail systems to the Systems Administrator upon request.

System Integrity

Computer viruses pose a significant risk to [Company]. Employees are therefore not permitted to use personal disks or copies of software on any [Company] computer without first obtaining specific authorization from the Systems Administrator. Any employee who introduces a virus into [Company]'s computer system may be deemed guilty of gross negligence and/or willful misconduct and may be held responsible for the consequences, including repair costs and other losses.

Similarly, information is not to be downloaded directly from the Internet onto [Company]'s computer system. If you need to download information from the Internet, you should download the data onto a disk and have the System Administrator scan the disk for viruses before introducing the data into [Company]'s system.

Enforcement

Violations of this policy may result in disciplinary action, including termination. Employees who damage [Company]'s computer system through its unauthorized use may additionally be liable for the costs resulting from such damage. Employees who misappropriate copyrighted or confidential and proprietary information, or who distribute harassing messages or information, may additionally be subject to criminal prosecution and/or substantial civil money damages.

Confidentiality

All records and files of [Company] are the property of [Company] and are considered confidential and proprietary. No employee is authorized to copy or disclose any file or record. Confidential information includes, but is not limited to, all letters or any other information concerning transactions with customers, customer lists, customer preferences, financial data, marketing strategies, product design information, research and development data, payroll or personnel records of past or present employees, financial records of [Company], all records pertaining to purchases from vendors or suppliers, correspondence and agreements with manufacturers or distributors and documents concerning operating procedures of [Company].