

**EMPLOYEE MISUSE OF EMPLOYER’S TECHNOLOGY**

**by Douglas E. Dexter**

**Chair, Employment Practice Group**

**Farella Braun + Martel LLP**

**San Francisco**

**TABLE OF CONTENTS**

I. Overview..... 1

II. Types of misuse ..... 1

    A. Company-related..... 1

        1. Harassment and threats ..... 1

        2. Misappropriation of trade secrets..... 2

        3. Fraud related to company operations..... 4

        4. Sabotage..... 5

        5. Copyright violations..... 7

        6. Obstruction of justice..... 7

        7. Other misuse ..... 8

    B. Dissemination of confidential information ..... 8

    C. Misuse directed outside the company ..... 9

III. Liability from misuse of technology..... 9

    A. Employer liability for its own misuse of technology..... 9

        1. Invasion of privacy ..... 9

        2. Electronic Communications Privacy Act, 18 U.S.C. §§2510-2712..... 10

    B. Employer liability to third persons for employee misuse of technology ..... 11

        1. In general ..... 11

        2. *Respondeat superior* ..... 11

        3. Ratification..... 12

        4. Negligent retention and supervision ..... 12

        5. Copyright violations..... 13

IV. Preventing problems ..... 13

    A. Examples of policies to be established in writing..... 13

    B. Monitoring e-mail, Internet, computer and telephone use..... 14

    C. Methods for protecting integrity of information systems and trade secrets..... 17

## EMPLOYEE MISUSE OF EMPLOYER'S TECHNOLOGY

by Douglas E. Dexter\*

### **I. Overview: Using the employer's technology**

- A. Technology such as telephones and datalines, computers and their networks, and Internet including e-mail, are now part of almost every American workplace – certainly of every workplace structured around an office environment, and increasingly of many that are not.
- B. It would be very hard for any employer to prevent employees from making some personal use of this technology. Even if this could be done, it would require diverting substantial resources to do it, and the cost in good will and workplace harmony would be huge. Rather than attempt this, most companies tolerate a certain level of personal use.
  - 1. The informal principle that workers may make some modest use of the employer's resources is at least as old as the Bible, where it is written: "Thou shalt not muzzle the ox when he treadeth out the corn." Deuteronomy 25:4.
- C. However, the risks to the employer of employee use of modern technology are not just the superficial ones of diversion of resources. Serious dangers, much intensified by the power of these technologies, arise in areas including but not limited to dissemination of trade secrets, debasement of the workplace by sexual harassment and other methods, company responsibility for employee torts (and even crimes such as securities fraud), and direct injury to the company through fraud, embezzlement and sabotage.
- D. To counter these risks, employers try to limit and monitor employees' personal use of company technology. Doing this sometimes brings employers into conflict with their employees and risks infringing their legitimate and enforceable privacy rights, and sometimes their labor rights as well.
- E. These materials focus on some of the issues raised by employee misuse of employer technology, and the management of the conflicts which can result.

### **II. Types of misuse**

#### **A. Company-related misuse**

- 1. Harassment and threats
  - a. Sexual harassment is often done through the employer's technology. See, e.g., *Cox v. State ex rel. Oklahoma Dept. of Human Services*, 87 P.3d 607, 618 (Okla. 2004) (multiple e-mails "rife with sexual innuendo" sent to female employees);

---

\* **Douglas E. Dexter** is a litigation partner in the San Francisco law firm of Farella Braun + Martel LLP and chair of its Employment Practice Group. He has spent more than 20 years advising employers on implementing sound business policies and on reducing the threat of employment litigation and workplace conflict, and has successfully represented employers before arbitrators, juries, administrative agencies and appellate courts on a variety of employment law issues. Doug Dexter can be reached at 415-954-4409, or by e-mail at [ddexter@fbm.com](mailto:ddexter@fbm.com).

*Hawk v. Americold Logistics, LLC*, 2003 WL 929221, \*4 (E.D.Pa.) (“unwelcome electronic ... communication of a sexual nature” delivered “regularly at work”).

- i. In *Edwards v. Ohio Institute of Cardiac Care*, 170 Ohio App.3d 619 (2007), a successful sexual harassment claim was based on a pattern of inappropriate e-mails from the company’s president to an employee.
  - ii. In *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 WL 974676 (D.Mass.), the offending action was not deliberate harassment but forwarding sexually explicit e-mails from internet joke sites to coworkers using the office system.
  - iii. In *Blakey v. Continental Airlines, Inc.*, 164 N.J. 38 (2000), the offensive material was posted on the employer’s electronic bulletin board. The court found this a “work-related forum” despite not being located physically within the workplace.
  - iv. In *Coniglio v. City of Berwyn, Illinois*, 2000 WL 967989 (N.D.Ill.), a male supervisor viewed Internet images of nude women on his office computer, within sight of female employees.
  - v. Examples could be multiplied.
- b. Recipients of offensive material need not be fellow employees for the conduct be detrimental to the company.
- i. For example, in *Autoliv ASP, Inc. v. Department of Workforce Services*, 29 P.3d 7 (Utah App. 2001), employees were properly terminated for sending offensive sexually explicit e-mails to a former employee, in violation of expressly stated company policies.
  - ii. In *Phillips v. American Family Ins. Co.*, 345 F.Supp.2d 1187, 1200 (D.Kan. 2004), not only did an employee send “numerous inappropriate and unwelcome sexually-oriented e-mails to his two female employees at the office,” but he also used the company’s “computer and e-mail to send sexually explicit photographs ... to persons throughout the local community,” which constituted conduct prejudicial to the company and grounds for termination.
- c. For a discussion of the use of employee e-mail in documenting gender discrimination see Lucille M. Ponte, “Victims of Gender Discrimination or Disgruntled Employees? The Evolving Role of Candid E-Mails in Gender Disparate Treatment Cases,” 19 Wisconsin Women’s Law Journal 47 (2004).
2. Misappropriation of trade secrets
- a. Trade secrets are often kept in electronic format.
    - i. “Employers’ greatest risk to their computer security comes not from outside hackers but from current and former employees who deliberately or inadvertently disclose confidential or sensitive information. According to a 2001 survey ... more than 40 percent of respondents admitted to receiving company confidential information such as client lists, financial statements and product specifications from outside their organizations – a 356 percent increase since 1999. Employees no longer have to photocopy documents

surreptitiously; they can simply download reams of data to disk, CD or DVD, or even e-mail the information to a competitor with the click of a mouse.” William G. Porter II and Michael C. Griffaton, “Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace,” 70 Defense Counsel Journal 65, 69 (2003) (internal quotation marks omitted).

- b. The Uniform Trade Secrets Act (“UTSA”), adopted in some form in most states, defines a trade secret as “information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” UTSA § 1(4); and *see, e.g.*, California Civil Code § 3426.1(d).
  - i. A California court has articulated this definition more economically as consisting “of three elements: (a) information (b) which is valuable because unknown to others and (c) which the owner has attempted to keep secret.” *ABBA Rubber Co. v. Seaquist*, 235 Cal.App.3d 1, 18 (1991).
- c. Trade secrets include not only proprietary information relating to a company’s product or service itself, but also information (such as confidential customer lists, marketing plans and pricing information) needed for selling it.
  - i. A company’s secret information about its “pricing, profit margins, costs of production, pricing concessions, promotional discounts, advertising allowances, volume rebates, marketing concessions, payment terms and rebate incentives ... has independent economic value because [it] would be valuable to a competitor to set prices which meet or undercut” their own. *Whyte v. Schlage Lock Co.*, 101 Cal.App.4th 1443, 1455 (2002).
- d. Thus, taking reasonable steps to ensure the secrecy of the information is an independent statutory element of trade secret protection.
  - i. Older cases and authorities often speak in terms of safes and locked compartments, and sign-out sheets for borrowed files. These methods are obsolete in the information age, but corresponding precautions have to be taken to protect electronic files. For example, in place of the locked safe, a special password should be required for access to trade secrets. In place of the sign-out sheet, access to secret information should be automatically logged.
    - (A) For a case in which trade secret protection was held not available because, among other things, computers containing the critical information were not password-protected and could be accessed by employees without restriction, *see Coleman v. Vukovich*, 825 N.E.2d 397, 405 (Ind.App. 2005).
  - ii. “If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.” *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984).

(A) When a secret is publicly disclosed “it loses any status it ever had as a trade secret.” *State ex rel. Lucas County Board of Commissioners v. Ohio Environmental Protection Agency*, 88 Ohio St.3d 166, 174 (2000).

(B) Note that the teaching of a patent, not being secret, cannot be a trade secret.

- e. Employers run risks that they may hire people who will unlawfully use their former employer’s trade secrets to further their careers with the new employer.
    - i. This kind of misappropriation, and various kinds of industrial espionage, are likely to involve an employer’s technology, and expose the benefiting company to liability.
  - f. Case examples
    - i. In *Telecom Technical Services Inc. v. Rolm Co.*, 388 F.3d 820, 832-33 (11th Cir. 2004), an employee took information from his former employer which could only have been accessed by means of wrongfully-acquired passwords. Evidence that access to “maintenance-level passwords” could only be had by using “higher-level engineering passwords” provided by the former employee was held sufficient to sustain a jury’s verdict of misappropriation of trade secrets.
    - ii. In *Northern Electric Co., Inc. v. Torma*, 819 N.E.2d 417 (Ind.App. 2004), a repair supervisor compiled technical data useful for diagnosing future malfunctions and formulating repair strategies, based on hundreds of repairs by company employees. He stored this information on his home computer and took it with him when he left for employment with a competitor, despite a demand for its return.
    - iii. In *People v. Eubanks*, 14 Cal.4th 580 (1997), a disaffected officer of a software company transmitted trade secrets to a competitor via commercial e-mail.
3. Fraud related to company operations
- a. Technology may be used to perpetrate a wide spectrum of offenses, including embezzlement, defrauding the company, defrauding customers, and corruption of company records (for example by padding sales numbers). Indeed, in the modern world it is hard to imagine any such scheme that did not require using the company’s information technology.
  - b. Technology often plays a role in the kind of misconduct that was prominent in the wave of corporate scandals which prompted the Sarbanes-Oxley reforms. Examples include:
    - i. Prematurely recognizing revenue, for example by posting as revenue sales which are not final, or transactions which are really only leases, or recognizing as revenue projected income from contracts subject to cancellation.
    - ii. Overvaluing goodwill, “managing” earnings and similar dishonest accounting.

- iii. Self-dealing by management.
  - iv. Giving or accepting kickbacks for orders.
4. Sabotage
- a. The easiest way for a modern office worker to sabotage the company is through its information technology. It only takes one disgruntled employee, or former employee with enough technical expertise, to create serious disruption which could last for an uncomfortable period of time and result in significant economic loss.
  - b. Stealing information or maliciously publicizing it has been discussed in Part II.A.2 under misappropriation of trade secrets.
  - c. An easier and more likely sabotage scenario is deleting or overwriting files.
    - i. Fortunately, technical means to prevent this are easy to implement, by restricting the files an employee has access to, or by reserving to IT management the ability to delete files (although it is hard to keep individual files from being overwritten). See Part IV.C below.
    - ii. Most companies maintain back-up and archival systems to recover files accidentally lost, and these work against deliberate sabotage also.
  - d. There are many other ways in which insiders or former insiders can attack company computers. One commentary distinguishes among *hacking* (gaining access to a computer or network without authorization, often just for the fun of it), *cracking* (gaining access for the purpose of committing another crime once inside), *sabotage* (gaining access for the purpose of doing damage), and *denial of access* or *spamming attack* (causing the system to be bombarded with so much unwanted information its capacity is temporarily degraded). See John J. Falvey, Jr. and Amy M. McCallen, 2 INTERNET LAW AND PRACTICE § 26:3 (2006).
    - i. The denial of access attack on Yahoo! in February 2000 is a famous example of this kind of incident.
  - e. A variation on sabotage by deletion is the deliberate saving, whether maliciously or otherwise, of documents intended to be destroyed under a document retention program.
    - i. The Microsoft antitrust case made this danger notorious and prompted many companies to use special software to delete stored e-mails automatically when they reach a pre-set age.
    - ii. Since people often need old e-mail files, and they can be demanded by investigators or discovery requests, provision has to be made to allow overrides, and this power can be used to defeat the retention policy.
    - iii. Michael Eisner told a graduating class at the University of Southern California that he had “come to believe that if anything will bring about the downfall of a company, or maybe even a country, it is blind copies of e-mails that should never have been sent in the first place.” For the full text of his entertaining remarks see the May 22, 2000 edition of the *USC Chronicle* – it is reprinted at

f. Case examples

i. In *United States v. Lloyd*, 269 F.3d 228, 231 (3d Cir. 2001), the defendant worked as a computer systems administrator for a manufacturer of highly specialized and sophisticated industrial process measurement devices and control equipment. Before his anticipated termination he planted a “logic bomb” in the central file server of the company’s computer network. It went off on a specified date after he left, permanently deleting the company’s design and production computer programs. It purged about 1,200 computer programs, crippling the company’s manufacturing capabilities and resulting in the loss of millions of dollars in sales and contracts.

(A) A similar event is discussed in *United States v. Sullivan*, 40 Fed.Appx. 740, 2002 WL 312773 (4th Cir. 2002). Sullivan set his logic bomb for four months after he quit, when it disabled 824 hand-held computers used by the company’s sales reps to communicate with headquarters.

ii. In *United States v. Middleton*, 231 F.3d 1207 (9th Cir. 2000), a former personal computer administrator at an internet service provider hacked into the system and changed all the administrative passwords, altered the computer’s registry, deleted the entire billing system (including programs that ran the billing software), and deleted two internal databases.

g. The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, criminalizes much of this activity. It specifically forbids intentionally accessing a “protected computer” without (or exceeding) authorization and thereby gaining information or aiding a fraud. It also applies when anyone “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer,” or under some conditions causes damage recklessly or otherwise, and in other circumstances.

i. The term “protected computer” was added to the law in 1996, to broaden its coverage. “As ‘protected computers’ includes those used in interstate commerce or communications, the statute now protects any computer attached to the Internet, even if all the computers involved are located in the same state.” Eric J. Bakewell and Michelle Koldaro, “Computer Crimes,” 38 *American Criminal Law Review* 481, 488 (2001) (footnotes omitted).

ii. The criminal side of this statute is beyond the scope of these materials, but it provides a private right of action in some situations. See 18 U.S.C. § 1030(g).

iii. Although the CFAA “allows recovery for losses beyond mere physical damage to property, the additional types of damages awarded by courts under the Act have generally been limited to those costs necessary to assess the damage caused to the plaintiff’s computer system or to resecure the system in the wake of a hacking attack.” *Tyco International (US) Inc. v. John Does I-3*, 2003 WL 21638205, \*1 (S.D.N.Y.).

## 5. Copyright violations

- a. Copyright infringement is probably the most common tort committed by employees using the employer's technology. It is committed every day in most large corporations, in the library and the copy room and in satellite copy stations, as employees create and distribute multiple copies of protected material in excess of fair use. E-mail is another potent vehicle for copyright infringement.
  - i. Questions of fair use and infringement are presented every time an employee makes multiple copies of a copyrighted document for circulation inside the company. It is rare that these questions are considered seriously, and as a result infringement liabilities routinely accumulate in the course of daily business. That the copyright owners usually do not know about these violations or try to enforce their rights does not make the infringements any less unlawful.
  - ii. As a practical matter there is little that can be done to stop this, and little likelihood of a company ever being brought to account for it. But it is worth mentioning as a classic example of how the miniaturization and wide dissemination of modern information technology has put its use beyond the practical ability of companies to control even if they want to.
  - iii. For a relatively rare example of a company actually being caught doing this and sued over it, see *Lowry's Reports, Inc. v. Legg Mason, Inc.*, 271 F.Supp.2d 737 (D.Md. 2003). Lowry's published a market letter which Legg Mason research employees routinely copied for internal distribution and at one point even posted on their intranet. Lowry's sued and won summary judgment for infringement; adjudication of enhanced damages for willfulness and for a separate claim of breach of the subscription contract was allowed to proceed to trial.

(A) "The fact that Legg Mason's employees infringed Lowry's copyrights in contravention of policy or order bears not on Legg Mason's liability, but rather on the amount of statutory and punitive damages and the award of attorneys' fees. Accordingly, unless Legg Mason can establish an affirmative defense, it is liable for the infringing conduct of its employees." *Id.*, 271 F.Supp.2d at 746 (citation omitted).
- b. Use and internal distribution of copyrighted computer programs beyond the scope of the license is another example of copyright infringement for which the company would be liable if caught.

## 6. Obstruction of justice

- a. Where there is a government investigation of any aspect of a company's operation, and employees try, out of motives of loyalty or self-preservation, to cover things up or hide or destroy documents, elements of obstruction of justice may be present which can multiply the consequences to the company of the original misconduct. As the original documents are often held electronically, any obstruction will likewise involve the company's technology.

- i. Obstructing even an internal investigation can trigger obstruction liability. In April 2004, for example, three former officers of Computer Associates, a software company, pleaded guilty to obstruction of justice, admitting that they lied to investigators during an internal company investigation focused on potential securities fraud issues. The prosecution theory was that, even though the defendants lied in a non-governmental inquiry, they knew their lies would be reported to federal investigators. See Alex Berenson, "Case Expands Type of Lies Prosecutors Will Pursue," *New York Times*, May 17, 2004.

7. Other misuse

- a. This by no means exhausts the possibilities for technology-related torts and even crimes for which the company may have some litigation exposure. They are limited only by the ingenuity of those with access to technology, which experience has shown to be almost boundless. Other examples include:

**B. Dissemination of confidential information**

1. Although usually not deliberate misuse in the sense used elsewhere in these materials, carelessness in dissemination of confidential information can still lead to undesirable consequences.
2. For example, legal advice, and requests for such advice, are privileged only as long as they remain confidential. E-mail makes broadcast dissemination of information so easy that people sometimes do not think before clicking. But forwarding (or attaching) an e-mail containing either a request for legal advice or the advice itself can vitiate privilege if disseminated beyond those who have both a need and a right to know.
  - a. For example, if legal advice about an accounting procedure is sent to everyone in the company's accounting group, the privilege will likely be lost. See, e.g., California Evidence Code § 952, limiting privileged disclosure to that "reasonably necessary for ... accomplishment of the purpose for which the lawyer is consulted."
    - i. Everyone with a need to know a decision or new procedure does not necessarily need to know the legal advice on which it is based.
  - b. If an e-mail with otherwise privileged attachments is sent to a third party, the privilege may be lost with respect to all the attached e-mails. See *United States v. ChevronTexaco Corp.*, 241 F.Supp.2d 1065 (N.D.Cal. 2002).
  - c. There are some steps that can be taken to reduce the risk.
    - i. As a matter of policy, lawyers (including in-house lawyers) should respond with legal advice only to the person who requests the advice.
    - ii. Advice or requests for advice should never be included in or attached to an e-mail with any other subject.
    - iii. The lawyer should routinely advise how widely to disseminate the response – legal advice or a request for it should be held as closely as possible.

(A) Who has a genuine need to know, rather than just an interest?

(B) Will communicating the decision be sufficient, or is understanding the legal basis really needed?

3. Even without privilege concerns, similar caution is required in disseminating personnel files, internal investigation documents, and other sensitive material about employees or others. Careless distribution, by e-mail or otherwise, can not only compromise company objectives but also impact privacy rights and expose the company to claims for invasion of privacy or even defamation.
  - a. As noted above, such caution is also needed with trade secret material such as marketing plans, customer lists and sales leads.

### **C. Misuse directed outside the company**

1. A wide variety of torts and crimes can be committed with computer, Internet, e-mail and telephone technology. Not all of them involve liability for the company even if committed using company equipment – in some cases the employee uses company technology because it is superior to his own, or because he believes it might help him evade detection. Every company should want to prevent use of its equipment for such purposes.
2. The following are just a selection of wrongs which can be committed using company technology. The same precautions outlined in Part IV, useful against wrongs involving the company, can discourage these as well, and aid in their detection.
  - a. Frauds of almost any nature, from Ponzi schemes to eBay swindles, involving computer files, Internet or e-mail.
  - b. Securities fraud, including but of course not limited to insider trading.
    - i. Use of the telephone in committing a fraud can make it wire fraud, a separate federal crime.
  - c. Defamation, trade libel, cybersmear, and other crimes against reputation – e-mail is an incubator for torts of this type.
  - d. Copyright violations not for the company's benefit, for example unlicensed downloading of music.
  - e. Computer trespass, hacking, spamming, and other electronic misdeeds when accomplished with the employer's technology.
    - i. Downloading of child pornography counts as a computer crime.
  - f. Wiretapping by unlawfully recording conversations.

## **III. Liability from misuse of technology**

### **A. Employer liability for its own misuse of technology**

1. Invasion of privacy
  - a. "One 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.” Restatement (Second) of Torts §652B (1965).

- b. When affirmative relief is sought to prevent an invasion of privacy, the plaintiff must establish “(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.” *Hill v. National Collegiate Athletic Assn.*, 7 Cal.4th 1, 39-40 (1994).
  - c. It is fairly well established that an employee does not ordinarily have a protectible privacy interest in communications on company equipment. Companies reinforce this through employee handbooks, splash screens, warnings on monitored phone lines, written acknowledgments executed on hiring and at annual reviews, and other similar means. See discussion in Part IV below.
  - d. “[T]he use of computers in the employment context carries with it social norms that effectively diminish the employee’s reasonable expectation of privacy with regard to his use of his employer’s computers.” *TBG Ins. Services Corp. v. Superior Court*, 96 Cal.App.4th 443, 452 (2002).
  - e. In *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 WL 974676 (D.Mass.), the court declined to find a reasonable expectation of privacy in e-mails sent on company equipment, which the employees knew would be accessible by third persons within the company.
2. Electronic Communications Privacy Act, 18 U.S.C. §§2510-2712
- a. In extreme cases the activities of an employer in monitoring employee communications could violate the Electronic Communications Privacy Act.
    - i. For a cautionary example, see *Smith v. Devers*, 2002 WL 75803 (M.D. Ala.) (manager monitoring employee’s personal telephone conversations).
  - b. This topic is beyond the scope of this paper. It is sufficient to note here that the law makes technical but important distinctions for telephones depending on equipment used, and for e-mail between interception of communications as they are made, and accessing of completed communications in storage. Company access to employee e-mails made on company equipment and stored after the fact on company equipment are unlikely except in rare circumstances to involve actionable invasions of employee privacy interests.
    - i. See, e.g., *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107, 114-115 (3d Cir. 2003) (applying to e-mails stored on company’s system the exception in 18 U.S.C. § 2701(c)(1) for retrieval of e-mail authorized “ by the person or entity providing a wire or electronic communications service”).
  - c. Any program involving monitoring or employee communications, or accessing their stored communications, should be undertaken only after consulting counsel. Procedures adequate to protect the company’s position can be devised before the fact more easily than ill-considered procedures can be defended after the fact.

## **B. Employer liability to third persons for employee misuse of technology**

### 1. In general

- a. Employer liability to third persons for misuse of its technology, although possible in theory, is usually difficult to establish in practice.
  - i. In the typical case the employee will have acted without the employer's knowledge, against its interest, and contrary to its policies.
  - ii. The traditional legal vehicles for fixing on an employer the liability for the torts of its employees usually exonerate the employer.

### 2. *Respondeat superior*

- a. "An employee acts within the scope of employment when performing work assigned by the employer or engaging in a course of conduct subject to the employer's control. An employee's act is not within the scope of employment when it occurs within an independent course of conduct not intended by the employee to serve any purpose of the employer." Restatement (Third) of Agency § 7.07(2) (2006).
  - i. In *Booker v. GTE.net LLC*, 214 F.Supp.2d 746 (E.D.Ky. 2002), aff'd 350 F.3d 515 (6th Cir. 2003), for example, Verizon employees sent discourteous responses to customer complaints, using someone else's e-mail address as a source. The true owner of that address sued the employees and Verizon. Because the employees were doing what they had been hired to do (responding to consumer complaints), the court found it a "close call," 214 F.Supp.2d at 750, but in the end held their conduct outside the scope of their employment.
- b. Restatement (Second) of Torts § 317 (1965) provides: "A master is under a duty to exercise reasonable care so to control his servant while acting *outside* the scope of his employment as to prevent him from intentionally harming others or from so conducting himself as to create an unreasonable risk of bodily harm to them, if the servant is upon the premises in possession of the master or upon which the servant is privileged to enter only as his servant, or is using a chattel of the master, and the master knows or has reason to know that he has the ability to control his servant, and knows or should know of the necessity and opportunity for exercising such control." (Emphasis added; subsection letters omitted.)
  - i. This section was central to the holding of employer liability in *Doe v. XYZ Corp.*, 382 N.J.Super. 122 (2005). There, through the vigilance of employees at or near the offender's level, the company was aware that its employee was surfing pornography sites. It had the policies in place to permit monitoring, and in fact a supervisor had noted use of a site seemingly directed toward child pornography. Nevertheless, despite being on notice and having the technical ability to follow up, the company declined to investigate or pursue the matter, and the employee used the company's technology to post improper photographs of his minor stepdaughter on an Internet pornography site. The court held the company liable in tort for the employee's misconduct.

### 3. Ratification

- a. Employer derivative liability for employee actions need not be founded on *respondeat superior*, but may be based upon the alternative doctrine of ratification. See, e.g., *Murillo v. Rite Stuff Foods, Inc.* 65 Cal.App.4th 833, 852 (1998).
- b. “An employer may be liable for an employee’s willful and malicious actions under principles of ratification. An employee’s actions may be ratified after the fact by the employer’s voluntary election to adopt the employee’s conduct by, in essence, treating the conduct as its own. The failure to discharge an employee after knowledge of his or her wrongful acts may be evidence supporting ratification.” *Delfino v. Agilent Technologies, Inc.*, 145 Cal.App.4th 790, 810 (2006) (citations omitted).
  - i. But in the *Delfino* case, where employees sent out threatening e-mails and bulletin board postings using the company’s technology, a ratification claim against the employer failed because for lack of evidence. The company had no knowledge of its employee’s improper actions, and when it learned of them acted at once to suspend and then discharge the offenders. See *id.*, 145 Cal.App.4th at 811.
  - ii. The court in *Delfino* also rejected *respondeat superior* liability, holding that the employees’ misconduct was outside the scope of their employment and so it would be contrary to the purpose of the doctrine to hold the employer responsible for it. See *id.*, 145 Cal.App.4th at 813-814.

### 4. Negligent retention and supervision

- a. “A principal who conducts an activity through an agent is subject to liability for harm to a third party caused by the agent’s conduct if the harm was caused by the principal’s negligence in selecting, training, retaining, supervising, or otherwise controlling the agent.” Restatement (Third) of Agency § 7.05 (2006).
- b. “An employer may be liable to a third person for the employer’s negligence in hiring or retaining an employee who is incompetent or unfit.” *Roman Catholic Bishop v. Superior Court*, 42 Cal.App.4th 1556, 1564 (1996) (citation omitted).
- c. Unlike the *respondeat superior* and ratification theories, negligent retention and supervision liability is direct and not vicarious. The existence of a duty to the plaintiff, and a failure of a reasonable standard of care in supervision, will usually be hard to prove.
  - i. For example, in *Chivers v. Central Noble Community Schools*, 423 F.Supp.2d 835, 856-7 (N.D.Ind. 2006), a third-party claim negligent supervision claim against a school district for a teacher’s improper Internet communications with a student was dismissed because the teacher’s conduct was not reasonably foreseeable.
  - ii. The *Delfino* case is again instructive, providing detailed analysis of the elements of a negligent supervision claim for unauthorized cyberthreats using employer’s technology. See *Delfino*, 145 Cal.App.4th at 815-818.

5. Copyright violations

- a. “Vicarious copyright liability is an outgrowth of *respondeat superior*. In the context of copyright law, vicarious liability extends beyond an employer/employee relationship to cases in which a defendant has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.” *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1022 (9th Cir. 2001) (citation and internal quotation marks omitted).
- b. See discussion in Part II.A.5 above.

**IV. Preventing problems**

**A. Examples of policies to be established in writing**

1. Prohibiting potentially harassing e-mail, internet or other computer use.
  - a. Use of company equipment for downloading or disseminating off-color or sexually oriented material, or racist material, may properly be forbidden.
2. Notification that workers have no privacy expectation in any technology provided by the company, including computer files, e-mails, Internet use, voicemail messages or business telephone conversations on company equipment, and that these may be recorded, monitored or examined at the company’s discretion.
  - a. This should include clarification that passwords do not imply privacy from the employer’s scrutiny.
  - b. Employees should be required to acknowledge that their consent to recording and monitoring of information and communications on the company’s systems is a condition of their employment.
  - c. There is case law to the effect that “[e]ven if [workers] had a reasonable expectation of privacy in their work e-mail, [the company’s] legitimate business interest in protecting its employees from harassment in the workplace would likely trump ... privacy interests.” *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 WL 974676, \*2 (D.Mass.). Other cases are in accord.
3. Prohibiting use of company equipment for copyright violations, including downloading of copyrighted material such as songs.
4. Affirming company ownership of all intellectual property, technical and marketing information, and the like. Periodically requiring that this be acknowledged by all employees can be a basis for claiming that reasonable measures were taken to protect trade secrets.
  - a. The company’s intellectual property, including both technical and commercial trade secrets, must be respected and protected against misuse or misappropriation both deliberate and inadvertent.
  - b. Inadvertent disclosures, for example of trade secrets, can be as dangerous as deliberate ones. The policy should aim at informing loyal but possibly careless employees as much as cautioning potentially faithless ones.

- c. Policies should also prohibit employees from using trade secrets owned by other employers.
  - i. Companies should require that new hires promise not to use prior employers' trade secrets in their work for the company.
- 5. Policies should include company rules (referring as well to state and federal laws) against accounting manipulations, and against securities fraud especially including insider trading.
  - a. Warnings against manipulation may be effective against employees who imagine that such conduct would be tacitly approved by the company.
  - b. Warnings against insider trading may be effective against employees who are exposed to inside information in the course of their work and who may not realize that trading on such information is illegal as well as forbidden.
  - c. Having these policies in place, and enforcing them promptly against transgressors, can help the company keep insulating distance between it and its offending employees in later negotiations with authorities.
- 6. The above listing by no means exhausts the universe of useful policies.

**B. Monitoring e-mail, Internet, computer and telephone use**

- 1. Monitoring e-mail and computer and Internet use is a common practice in American offices.
  - a. A 2001 survey by the American Management Association showed about 76% of major U.S. corporations monitoring employee Web connections. For e-mail, 55% retain and review employee messages. For storage and review of e-mail only, the average was around 46%. And 36% track content, keystrokes and keyboard time. These figures have increased since the previous study four years before. See American Management Association, "2005 Electronic Monitoring and Surveillance Study," a précis of which is on the Web at [www.amanet.org/press/amanews/ems05.htm](http://www.amanet.org/press/amanews/ems05.htm).
    - i. "Of those organizations that engage in monitoring and surveillance activities, fully 80% inform workers that the company is monitoring content, keystrokes and time spent at the keyboard; 82% let employees know the company stores and reviews computer files; 86% alert employees to e-mail monitoring; and 89% notify employees that their Web usage is being tracked." *Ibid.*
    - ii. Of the employers whose policies were reported on in this study, 84% have established policies governing personal e-mail use, 81% for personal Internet use, 42% for personal instant messaging, 34 for operation of personal Web sites on company time, 23% for personal postings on corporate blogs, and 20% for operation of personal blogs on company time. See *ibid.*
  - b. Monitoring methods include *direct surveillance*, which records periodic "snapshots" of workers' screens, *keystroke logging*, which as its name implies allows reconstruction of every computer action, and *keyword flagging*, which alerts management to use of specific words in e-mail or Internet searches.

- i. Keyword flagging is useful not only for locating sexually or racially oriented material but also for tracking the company's proprietary information.
  - ii. Software for all these purposes is commercially available, and consultants are able to provide monitoring at almost any level of detail required.
- 2. Courts generally recognize that a company may access e-mail stored on its own system for business purposes, especially after a warning has been given. See, e.g., discussion in *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3d Cir. 2003).
  - a. "U.S. law gives employees few protections against employer surveillance of their workplace communications. Even without express employee consent, U.S. employers generally may listen to workplace telephone conversations, read messages sent to and from corporate e-mail accounts, and record and disclose the contents of employee communications. Employees that bring legal challenges to these practices rarely succeed in U.S. courts." Charles H. Kennedy and Trisha Kanan, "Surveillance of Workplace Communications: U.S. Employer Rights," 4 Privacy and Information Law Report No. 7, at 1 (March 2004).
    - i. "Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim. The laptops were Glenayre's property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common . . . that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible." *Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002) (citations omitted).
    - ii. Express consent can also be enforced to access company-related information on a home computer.
      - (A) "TBG's advance notice to Zieminski (the company's policy statement) gave Zieminski the opportunity to consent to or reject the very thing that he now complains about, and that notice, combined with his written consent to the policy, defeats his claim that he had a reasonable expectation of privacy. Several months after Zieminski started using the home computer, he signed TBG's policy statement, thereby acknowledging his understanding that the home computer was 'the property of the Company' and, as such, 'to be used for business purposes only and not for personal benefit or non-Company purposes.' He agreed that the computer would not 'be used for improper, derogatory, defamatory, obscene or other inappropriate purposes,' acknowledged his understanding that 'communications transmitted by Company systems [were] not considered private,' and consented to TBG's designation of 'authorized personnel to enter such systems and monitor messages and files on an 'as needed' basis.' He was notified that this monitoring could 'include the review, copying or deletion of messages, or the disclosure of such messages or files to other authorized persons.' His signature shows that he read TBG's policy, understood it, and agreed to adhere to it." *TBG*

*Ins. Services Corp. v. Superior Court*, 96 Cal.App.4th 443, 452-453 (2002).

3. Awareness that their e-mail and computer and Internet use are monitored by the company, and constant reminders by techniques such as splash screens, will have a definite, if immeasurable, deterrent effect on misuse.
  - a. Workers should be made to realize that they are in effect copying their supervisors on all e-mails, and that their supervisors are in a position to know if they access pornography on the job.
  - b. A splash screen notice made the difference in *United States v. Bailey*, 272 F.Supp.2d 822, 831 (D.Neb. 2003). The court decided there was no reasonable expectation of privacy because on each opening of the system, “[b]efore any password login screen appeared, the computer screen displayed the following notice: These computer resources are solely owned by the Company. \* \* \* Your use of this computer system is consent to be monitored and authorization to search your personal computer to assure compliance with company policies.”
4. Different standards apply in monitoring telephone conversations and retrieving phonemail.
  - a. The variation of state wiretapping laws, and the federal Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*, make telephone and phonemail monitoring a difficult and sensitive area.
    - i. Outcomes can turn on such technical points as whether the recording device is part of the original telephone equipment. See, e.g., *Williams v. Poulos*, 11 F.3d 271, 280 (1st Cir. 1993) (alligator-clip recording device did not qualify for statutory exception as component of telephone equipment).
    - ii. The number of parties and form of consent necessary varies from state to state.
  - b. The sufficiency of announcements to justify monitoring of personal calls is uncertain. For example, in *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir. 1983), the court held that “knowledge of the capability of monitoring alone cannot be considered implied consent” and that consent will be implied only when the employee knew or should have known of a policy of *constantly* monitoring calls, or when the employee conducts a personal conversation over a line that is *explicitly* reserved for business.
    - i. But compare, e.g., *United States v. Rittweger*, 258 F.Supp.2d 345, 355 (S.D.N.Y. 2003), distinguishing the situation where an employee knew that phone lines in a particular area were continuously taped and that the company reserved the right to listen to the tapes.
  - c. Any employer contemplating a telephone monitoring program should involve counsel in structuring it so as to be certain the program stays within the law.

## 5. NLRB Issues

- a. Company regulations and restrictions on employee use of technology must be carefully drawn and administered so as not to violate labor laws. For example:
  - i. In *Register-Guard*, 2002 WL 336963 (NLRB Div. of Judges), a company communications policy discriminatorily applied against union-related communications was held unlawful.
    - (A) As the Judges said, “If an employer allows employees to use its communications equipment for non-work related purposes, it may not validly prohibit employee use of communications equipment for Section 7 purposes.”
    - (B) In *Prudential Insurance Company of America*, 2002 WL 31493320 (NLRB Div. of Judges), the company’s policy of prohibiting employees from using the company e-mail system to communicate with each other about union-related matters was overly broad, and interfered with employees’ exercise of their rights under § 7 of the NLRA.
  - ii. In *St. Joseph’s Hospital*, 337 NLRB 94 (2001), a company rule forbidding a nurse from putting a pro-union message on her work-station computer screen-saver, and a warning to her for doing so, were ordered rescinded as violative of NLRA § 8.
  - iii. Examples could be multiplied.

### **C. Methods for protecting integrity of information systems and trade secrets**

1. One method is to compartmentalize access on a need-for-use basis, so that most people do not have access to all areas of the company’s system. If an employee needs access to an area beyond her ordinary responsibilities it can be given by means of a temporary password which can be de-activated after the need has passed.
  - a. Special passwords can be made individual, so as to reveal which employee (rather than just which computer) accessed which information. Special access passwords can be changed from time to time, especially when a key employee leaves, and a “two-key” system can be required for access to secrets of special importance.
    - i. The two-key system is modeled on the military protocol for firing missiles. To avoid unauthorized action, two officers must use their keys simultaneously for the missile to launch. Likewise a rogue saboteur cannot secretly delete critical files if another responsible employee must concur at the moment of deletion.
  - b. In addition a company might impose automatic restrictions on sending of given files by e-mail or otherwise, monitor (and/or block transmission) of e-mail with selected keywords, or take other similar measures.
  - c. Likewise all a company’s trade secrets should not be available using the same password – access should be compartmentalized on a need-to-know basis.
    - i. It is unlikely, for example, that the same person will need access to source code and customer lists.

- ii. Similarly a person who may need to know some part of a technical trade secret may not need to know every part.
  - iii. Access to secret information should be automatically logged by password, so it can be determined on a real-time basis who has accessed it, and unusual or suspicious patterns can be detected quickly.
  - iv. There is a tradeoff between compartmentalization of information and efficiency of operation. The right mix is a policy decision to be taken by executive management, in consultation with counsel, IT managers, and the line managers who run the operations whose efficiency may be impaired.
2. Trade secrets and computer security information should not be transmitted by fax, and should be transmitted by e-mail attachment only very sparingly, for good reason, and with careful precautions.
  3. Passwords should be de-activated instantly when an employee quits, or is terminated or suspended. This will not prevent every abuse – the employee in *United States v. Lloyd*, 269 F.3d 228 (3d Cir. 2001), mentioned above, apparently set his logic bomb when he expected termination but it had not yet happened. But it can help.
  4. The company’s array of security measures – firewalls, encryption, encrypted log-in, and anti-virus and anti-worm software, should be vigilantly maintained and periodically reviewed and reset.
  5. Periodic unannounced checks of offices, computers, PDAs and e-mails will reveal material which shouldn’t be there, and other suspicious circumstances.
  6. Any company would do well to review its information security needs periodically with an outside consultant. This allows for an independent viewpoint, expert guidance, and a measure of insulation from insiders whose potential treachery is one reason elaborate measures are needed.
  7. Although the computer is the way most information is now maintained and accessed, the copier needs attention also. Examples of precautions here might include having all copying of sensitive proprietary or security information done by a dedicated employee who logs what is copied and by whom, and having secret documents printed in blue ink or on special blue paper which resists copying.
    - a. Other paper-based methods include use of a secrecy stamp and shredding secret material no longer needed (including drafts and interim material and material copied for a completed purpose).
  8. A Latin maxim inquired: who will guard the guards? *Someone* needs to have total access to run the company’s computer systems, and in several cases that person has been the one who turned saboteur after leaving. No precautions can protect completely against betrayal by a trusted administrator. But some can help.
    - a. When a high-access employee leaves under less than friendly conditions the computer security safeguards and access protocols should be reset immediately to forestall tampering.

- b. A two-key system could be required for potentially harmful actions like deleting critical files, so as to limit the amount of damage an individual employee can do.
    - i. Perhaps a critical element of the security system could be left under the control of an outside consultant rather than an employee.
  - c. “Clean-up” operations such as that in *Lloyd*, where the IT administrator planning the logic bomb sabotage first recalled duplicate and back-up copies from elsewhere in the company, should not be ordinarily be permitted, or ever permitted with the involvement of only one administrator.
  - d. Some commentators suggest imposing a rule forbidding employees to use company computers at home. But this conflicts with the other recommendations that employees working at home be *required* to use company computers so as to defeat privacy claims. And forbidding use of company computers at home only fosters the spread of company information outside company systems.
9. A company’s employees are not the only ones who may seek to acquire company secrets. Anti-espionage techniques should be studied and applied – there are consultants with the expertise to do this. Anti-hacking protection is also part of a counter-espionage program.
10. Finally, a policy of referring for criminal prosecution violations of the CFAA or laws against theft of trade secrets should be announced, publicized, and vigorously enforced for its deterrent effect.

October 2007