STAFFORD FREY COOPER

DEVELOPING EMPLOYMENT POLICIES FOR E-MAIL, CELL PHONES, INSTANT MESSAGING, AND TEXT MESSAGING[1]

By Danford D. Grant

Danford D. Grant is a shareholder at Stafford Frey Cooper, P.C. in Seattle. His practice focuses on business torts and privacy, including disputes related to data loss and the disclosure of confidential information. Dan has lectured on a variety of privacy, employment, and procedural issues and has published articles related to privacy law and other matters. He has been recognized by his peers as a "Rising Star" in *Washington Law & Politics* magazine. Dan is a member of the International Association of Privacy Professionals (IAPP). He earned a J.D. from the University of Kansas School of Law where he was elected *Order of the Coif*, and an LL.M. from the University of Washington. Dan is admitted to practice in all Washington state courts, in the United States District Courts in both the Western and Eastern districts of Washington, and in the United States Court of Appeals for the Ninth Circuit.

[1] These materials should not be construed as legal advice, but only as general information about the law. Legal advice can only be given after analyzing the issues in response to specific information from a client.

I. Introduction

As we discussed during last year's presentation, businesses have important reasons to protect private and confidential information. Securing business information preserves trade secrets and other intangible assets, and protecting customer information creates trust and brand loyalty, reduces litigation, and prevents liability. In addition, the spread of misleading and inaccurate information through email, text and instant messaging, and the Internet can damage a company's reputation. Despite this need, controlling the flow of information poses technical, legal, and social-behavioral challenges for businesses. Email, text messages, instant messages, peer-to-peer (P2P) file sharing programs, unauthorized software downloads, and even the use of cell phones, home computers, and web-based email for work related projects, all expose business data and jeopardize information security.

Notwithstanding these challenges, businesses must create, implement, and follow an effective technology and information security policy. Many of us have heard dramatic stories about data loss in recent years, and messaging devices—especially instant messages through P2P networks—are often a culprit contributing to the loss of confidential information. Thus, one of the most important avenues for protecting business and customer information is an employer's ability to control and monitor employee electronic messaging devices.

For context, these materials provide background information regarding employee privacy rights that impact an employer's ability to monitor and control employee messaging. They discuss an employer's legal ability to monitor an employee's devices, including cell phones, email, and instant messaging. Finally, these materials highlight policies designed to permit monitoring and protect information from accidental or intentional disclosure.

II. Employee Privacy Rights

A. Generally

Privacy at work is limited. *See G.M. Leasing Corp. v. United States*, 429 U.S. 338 (1977); *see also O'Connor v. Ortega*, 480 U.S. 709 (1987).

An employee's right to privacy at work depends on the employee's "reasonable expectation of privacy," *id.*, which depends in large part on the identity of the intruder and the means of the intrusion. *Sanders v. American Broadcasting Companies*, 20 Cal.4th 907, 911, 85 Cal.Rptr.2d 909, 978 P.2d 67 (1999). When the "identity" of the intruder is the employer, and when the means of the intrusion is clearly disclosed to the employee in advance of the intrusion, the intrusion is usually legal. Thus, employment policies that give notice of an employer's monitoring methods are critical to an effective monitoring program.

B. Sources of Employee Privacy Rights[2]

1. Private Employees

- Privacy torts
- Washington Privacy Act
- Federal Wiretap law and the ECPA
- ADA and state statutes
- Contract
- California Constitution

2. Public Employees

- All of the above, PLUS
- Fourth Amendment
- 14th Amendment - Substantive Due Process (*Whalen v. Roe*)
- State Constitutions (Wash. Const. Art. 1, Sec. 7)

C. The Nature and Scope of Employee Privacy Rights

The nature and scope of an employee's right to privacy depends in part on whether the employer is a public or private entity.

1. Public Employers

Public employees have more privacy protection than private employees because the constitution protects privacy rights and applies to government employers. The standard applicable to public workplace monitoring declares that monitoring must be *reasonable under all the circumstances*. *O'Connor v. Ortega*, 480 U.S. 709, 725-26 (1987). The Court reasoned that "[a] reasonableness standard permits regulation of the employer's conduct according to the dictates of reason and common sense." Although adaptable, this standard is unrevealing and difficult to rely on for guidance.

To determine if monitoring is "reasonable" in the government context, courts use a two-pronged threshold test to determine first if an employee has a right of privacy in the government workplace. The court determines if the employee has an actual expectation of privacy (subjective test), and then determines if the expectation is reasonable (objective test).[3] Then, once the court concludes that the employee has a reasonable expectation of privacy, the court "...balance[s] the invasion of the employee's legitimate expectations of

[2] This is not an exhaustive list, but merely an example of some of the more common sources.
[3] An employee's reasonable expectation of privacy is reduced where the employer informs the employee in advance that he or she will be subject to monitoring. *Biby v. Board of Regents of University of Nebraska at Lincoln*, 419 F.3d 845 (8th Cir. 2005).

privacy against the government's need for supervision, control, and the efficient operation of the workplace." *See O'Connor v. Ortega*, 480 U.S. 709, 719-20 (1987).

The U.S. Court of Appeals for the Second Circuit (in New York) has developed a two-part test to evaluate the reasonableness of monitoring intended to uncover employee misconduct. According to the court, "[a]n investigatory search for evidence of suspected work-related employee misfeasance will be constitutionally "reasonable" if it is [1] justified at its inception, and [2] of appropriate scope." *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001). A search is "reasonable at inception" if "there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct." A search is "of appropriate scope" if it is "reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct."

Finally, any person (including a public employee) can waive constitutional protections if the waiver is "knowing, intelligent, and voluntary." *Schriro v. Landrigan*, 127 S.Ct. 1933, 1946 (2007). Thus, an employee can consent to an otherwise unreasonable search. *See McDonell v. Hunter*, 809 F.2d 1302 (8th Cir. 1987). Notably, however, a government employer cannot require an unreasonable search as a condition of employment. *See Pickering v. Board of Education*, 391 U.S. 563 (1968). Therefore, an employer probably cannot terminate an employee for refusing to consent to an unreasonable search.

2. Private Employers

In Washington, there is no constitutional right of workplace privacy for private sector employees. *See Roe v. Quality Trans. Servs.*, 67 Wn. App. 604, 838 P.2d 128 (1992). Thus, private employers are less restricted than public employers in their ability to monitor their employees.[4] Nevertheless, private employees are still protected. A private employer must avoid highly offensive invasions of an employee's reasonable expectations of privacy to protect itself from a common law invasion of privacy claim. *See Doe v. Gonzaga Univ.*, 143 Wn.2d 687, 705-06, 24 P.3d 390 (2001) (*rev'd on other grounds by* 536 U.S. 273, 122 S.Ct. 2268 (2002)). Private employers must also comply with any express or implied contractual obligations, and various statutes that protect against specific behaviors or protect specific types of information. For example, the Wiretap Act protects against the interception of electronic communications.

Despite wider latitude for private employers, an employee's reasonable expectation of privacy can still interfere with a private employer's ability to search. *See K-Mart v. Trotti*, 677 S.W.2d 632 (Tex. App. 1984). In *Trotti*, a K-Mart store manager and three assistants searched employees' lockers because

[4] Notably, this is not true in California because the California constitution applies to both public and private employers.

store security personnel suspected that an employee had stolen a watch. In addition, the store manager suspected an employee had stolen missing price guns. Employee Trotti used a personal lock to secure her purse and other belongings inside her locker. During an afternoon break, she returned to her locker and found the lock hanging open and personal items from her purse in disorder. Trotti sued K-Mart, claiming invasion of privacy. A jury awarded $8,000 in actual damages and another $100,000 in punitive damages. Although the court of appeals reversed on other grounds (a defect in the jury instructions), the court nevertheless found that Trotti had a reasonable expectation of privacy in her locker, that K-Mart had invaded that privacy interest, and that the jury's $100,000 award was not excessive under the circumstances. Specifically, the court held that an employer cannot search the locker of an employee when the employee expects privacy in the locker after providing her own lock at her own expense and with the employer's consent.

III. Monitoring and Surveillance of Employees

A. Monitoring Generally

Employers that want to monitor their employees should make sure their employees know the employer can and will search, and the best way to do this is through a clear and effective employment policy. Although employers use a variety of methods to monitor their employees, including drug tests, credit reports, medical reports, private investigators, psychological tests, polygraph tests, questionnaires, office searches, video surveillance, and GPS or other electronic tracking devices, this presentation will focus on an employer's right to monitor email, cell phones, text messages, and instant messages.

B. The Duty to Monitor Employees

Monitoring employees is good business, and in some situations it may be required. Furthermore, there is at least a general duty to supervise all employees, and the duty to supervise might include the duty to monitor, especially when an employer has notice of prior or ongoing misconduct. *See e.g., Doe v. XYC Corp.*, 887 A.2d 1156 (N.J. Superior Ct. App. Div. 2005); *see also*, *Does 1 - 9 v. Compcare, Inc.*, 52 Wn.App. 688, 763 P.2d 1237 (1988).

In *XYC Corp.,* a network administrator discovered that an employee was accessing pornography on his work computer. Supervisors told the employee to stop and the employee said he would comply with their demand. Later the employee used his work computer to upload nude photos of his daughter (a minor child) to the Internet. The mother of the child victim (and wife of the employee) sued the employer on behalf of the child, alleging that the employer knew or should have known and that it had a duty to report the employee's behavior to authorities. The court held:

> … an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third parties.

Doe v. XYC Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005). This opinion is unusual, and puts the employer in a law enforcement role, but it may reflect an extension of the modern trend toward a duty to monitor (instead of merely a right to monitor).

On a more basic level, adequate security measures—which include effective monitoring—are necessary to protect a company's trade secrets and intangible assets. Trade secrets lose their status as protected secrets when the business that owns the secret fails to take adequate measures to maintain and protect the secret. Although a discussion of trade secrets is well beyond the scope of these materials, a company should not ignore its own policies and procedures intended to protect electronic messages and claim it has information security measures adequate to preserve trade secrets.

C. Restrictions on Monitoring Electronic Messages

1. Generally

Although the law may be moving toward a more prominent duty to monitor employees, the ability to monitor is not without limits. Specific statutes and the common law provide various protections to employees in certain circumstances. Below are some of the more common employee protections related to telephones, emails, and other messages.

2. Searching Computer Files

An employer that owns a workplace computer and maintains control over the computer (including a computer used by an employee) can search the computer. The employer also has the authority to consent to a search of the computer by law enforcement. *See United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007). In *Ziegler*, an employee of a private company accessed Internet child pornography from his work computer located in his personal office. The employee's office was locked and his computer was password protected. The employee did not share the computer with anyone. When the employer learned that the employee was accessing child pornography using the computer, the employer contacted the FBI and then cooperated with the resulting criminal investigation. In the course of cooperating, the employer consented to a search of the computer and the government found the child pornography. The employee then tried to suppress the evidence in his criminal trial.

The court held that an employer can consent to a search of an employee's workplace computer. Although the employee maintained a reasonable expectation of privacy in his workplace office and computer because of the lock and the password, the employer nevertheless retained the ability to consent to the search because the office and computer were workplace property that remained under the control of the employer.

3. Monitoring Emails

The Electronic Communications Privacy Act of 1986 prohibits the interception, use, or disclosure of electronic communications under certain circumstances. Under the Wiretap Act (in effect for decades but since 1986 included as a chapter of ECPA), employers cannot "intercept" email unless it falls within an exception. The exceptions in the Wiretap Act relevant to employer email monitoring are (1) consent and (2) an interception in the ordinary course of business. Notably, however, "stored" email is not "intercepted," and therefore email in storage is controlled by the Stored Communications Act (another chapter of ECPA). Email on the employer's server is arguably "in storage." *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994). Pursuant to an exception in the SCA, an employer can access email in storage if the employer is the Internet or email service provider, or perhaps even if the employer is an authorized agent of the Internet or email service provider.

The first exception—consent—is the most relevant to our discussion because employer policies can establish consent.

In *Biby v. Board of Regents of University of Nebraska at Lincoln*, 419 F.3d 845 (8th Cir. 2005), the court held that an employer did not violate an employee's privacy when searching the employee's computer for emails relevant to a pending arbitration. The employer's computer policy specifically told employees that computer files, including email, could be searched in response to a discovery request in the course of litigation. In light of this policy, the court found that the employee had no reasonable expectation of privacy in his computer files under the circumstances. The court also rejected the argument that the policy allowed unreasonably broad searches, concluding that the employer needed to search broadly to ensure it had gathered all discoverable documents.

In *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), an at-will employee brought suit against an employer alleging wrongful termination and invasion of privacy. The employer fired the employee after intercepting an email the employee sent a supervisor complaining about co-workers and management. Notably, the employer had previously assured employees that email could not be inspected and would not be used as a basis for termination. Nevertheless, the court held that an employee has no reasonable expectation of privacy in emails he sends to other employees over the company system, *even when the company repeatedly assures employees that email will not be intercepted or read and used*

as a basis for termination. Although this decision is questionable based on the employer's representations, it illustrates the wide latitude employers have to monitor employee email use.

In *McLaren v. Microsoft Corp.*, 1999 WL 339015 (Tx. App. 1999) (unpublished), Microsoft suspended an employee while investigating accusations of sexual harassment and "inventory questions." The employee asked for access to his email to refute the allegations against him, but was told he could only access messages by telling company officials the locations of the specific messages he sought. General access to the email system required a network password. The employee also had a "personal store" to protect his personal emails, and asked that no one tamper with his workstation or email. After being terminated, the employee sued Microsoft for invasion of privacy, claiming the company had decrypted, "broken into," and released the contents of his personal folders to third parties. Distinguishing the court decision regarding the lockers in *Trotti*, the court held the employee had no reasonable expectation of privacy in his computer or emails. Unlike a locker, whose purpose is to store *personal* items, Microsoft provided computers to employees so they could perform the functions of their jobs. Additionally, email transmitted through a network is accessible by third parties, even if the employee later stores the email in a password-protected personal folder. Thus, the court concluded that the employee could not manifest–and Microsoft did not recognize–a reasonable expectation of privacy in files stored on his computer workstation. Moreover, the court concluded that even if the employee had some expectation of privacy, Microsoft's invasion of that privacy was not "highly offensive" and therefore could not give rise to legal liability. Notably, however, the court reached this conclusion without discussing Microsoft's computer use policy.

In *U.S. v. Simons*, 206 F.3d 392 (2000), the CIA's Foreign Bureau of Information Services (FBIS) monitored employees for any violations of the FBIS Internet usage policy which required employees to limit their Internet use to official government business. The policy also informed employees that the FBIS would audit and monitor Internet use. When a firewall test indicated an employee's computer was used to visit non-work-related websites, supervisors used a remote workstation to examine the contents of the employee's computer, including his Internet usage and downloads. They found over 1,000 downloaded pictures, and the several samples they viewed were pornographic. The employer then copied all the files on the employee's computer from a remote workstation. A criminal investigator from the CIA viewed selected files and discovered they were pornographic pictures of minors. The employer then physically entered the employee's office, removed his hard drive, replaced it with a copy, and gave the original to the FBIS Area Security Officer, who gave it to the criminal investigator. An FBI agent later viewed over 50 images on the hard drive, many that contained child pornography. The agent then obtained a search warrant to search the employee's office and computer. When agents executed the warrant, they copied the contents of employee's computer, diskettes found in his desk drawer,

computer files on a zip drive connected to his computer, videotapes, and a number of documents. In the employee's subsequent criminal prosecution, the employee sought to suppress the pornographic pictures, claiming they had been discovered in a search and seizure prohibited by the Fourth Amendment. First, the court concluded that the employee had no reasonable expectation of privacy in his computer because of the employer's computer policy. Next the court concluded that although the employee had an expectation of privacy in his office, which he did not share, the employer's entry to retrieve the hard drive was a reasonable workplace search because "FBIS had an interest in fully investigating [the employee's] misconduct...."

In *TBG Ins. Services Corp. v. Superior Court*, 96 Cal.App.4th 443, 117 Cal.Rptr.2d 155 (2002) an executive-level employee used two computers owned by his employer, one at the office and one at home. According to the employee, the home computer was a perk given to every executive and it was universally accepted that such computers could be used for both personal and business purposes. However, the employee had signed an electronic and telephone equipment policy agreeing that his computers could be used only for business purposes, the company could monitor his computers on an "as needed" basis, and communications using his computers were not private. The company fired the employee after discovering he had repeatedly accessed pornographic websites at work. The employee claimed that he did not intentionally access the sites, but they simply "popped up" on his computer. He also argued that the company's allegations of pornography were a pretext and he had been fired to prevent the vesting of company shares three days later. When the employee sued for wrongful termination, the employer served a discovery request for the home computer. Although the court found the employee had privacy interests in personal information he kept on the home computer (e.g. finances, family communications), it also noted that "the 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." Thus, the court concluded that when the employee signed the equipment policy, the employee had the opportunity to consent to or reject the invasion he now challenged, and he had therefore waived whatever privacy right he may have had in the home computer. The court therefore ordered production of the home computer, but also stated that the employee could ask to exclude specific information from discovery.

IV. Recommended Policies and Practices

A. Best Practices Generally

As the Supreme Court noted in *O'Connor v. Ortega*, 480 U.S. 709, 725-26, "[employee e]xpectations of privacy … may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." A messaging policy notifying an employee that the employer will monitor messages will reduce or

eliminate an employee's expectation of privacy in his or her messages. Notice that an employer will monitor email and Internet activity will reduce expectations of privacy in email and Internet activity. Thus, to effectively monitor employees, an employer should formulate a policy that informs the employee that it will (or at the very least reserves the right to) monitor messages, email and computer use.

B. Policies with Regard to Computer Messaging

1. Email and Internet Use

As noted above, whether monitoring is allowed turns on an employee's reasonable expectation of privacy. Providing notice of monitoring will typically reduce or eliminate an expectation of privacy in email, Internet use, computer files, and text messages.

All email and computer monitoring should be fair and consistent with the disclosed policy. At a minimum, employers should adopt the following policies and procedures regarding email use:

- Give prominent notice that email is subject to monitoring;
- Save incoming and outgoing email and review it from storage, instead of intercepting its transmission;
- Establish an email retention schedule and comply with it;
- Train employees that prohibitions on discriminatory and harassing behavior apply to email;
- Train employees not to send or discuss trade secrets over email;
- Prevent disruptive emails.

2. Instant Messaging

See attached materials

C. Policies with Regard to Cell Phones and Text Messaging

1. Cell Phone Use

See attached materials

2. Text Messaging

See discussion of *Quon v. Arch Wireless Operating Company*, 529 F.3d 892 (9th Cir. 2008) and other attached materials.