

HALL | FARLEY

HALL, FARLEY, OBERRECHT & BLANTON, P.A.

Private Sector Employees' Limited Right To Privacy In Their Personal Use of Employer-Provided Computer Equipment and Services

By Sarah A. Arnett

Inevitably, employees take advantage of their access to employer-provided computer equipment, e-mail systems, and Internet access. As a practical matter, you expect that your employees will make some personal uses of employer-provided computer equipment, systems, and services. Employees' personal uses frequently amount to nothing more than socializing with co-workers, friends, or family using employer-provided e-mail systems or paying personal bills and doing routine shopping using employer-provided Internet access. Unfortunately, however, there are employee abuses of employer-provided computer access which can lead to loss of revenue and legal liability for your business. Employee abuses can consist of excessive personal use of employer-provided e-mail systems and Internet access, which results in decreased productivity. Employees can also abuse their computer access by using inter-workplace e-mail to perpetrate discrimination or harassment against other employees, or by using Internet access to make unauthorized disclosures of proprietary information, or even to engage in criminal activities such as downloading child pornography. These sorts of unlawful activities can expose your business to legal liability.

You clearly have a considerable business interest in monitoring your employees' uses of the workplace computer systems and Internet access which you provide. But do employees have a right to privacy in their personal communications, files, and Internet activities on employer-provided computer systems? You need to be aware of the federal and state laws which provide some privacy protections to employees. Fortunately, courts have significantly limited the application of those laws by recognizing your considerable interests in protecting your businesses from employee abuses of employer-provided computer systems and Internet access.

Claims Which Can Be Brought By Private Sector Employees

In Idaho, if a private sector employee claims his or her employer has wrongfully obtained personal e-mail messages or other electronic files containing personal materials, he or she may seek relief under federal and Idaho statutes prohibiting unauthorized accessing of electronic communications, and under Idaho tort law prohibiting invasion of personal privacy. As yet there are not many cases in which courts have applied these laws to claims involving employer access to electronic files containing employees' personal materials. Fortunately, in those cases where such claims have been addressed, courts have come out strongly in favor of private sector employers when employees claim a right to privacy in personal e-mail messages and other electronic files stored on an employer-provided computer system.

Federal and Idaho Legislation Protecting Privacy in Electronic Communications

In 1986, the U.S. Congress passed the Electronic Communications Privacy Act (“ECPA”), which provides privacy protection in electronic communications. Title I of the ECPA, 18 U.S.C. §§ 2510-2522, amended existing federal legislation, known as the federal Wiretap Act, which had previously addressed only wire and oral communications. The federal Wiretap Act prohibits intentional unauthorized “interception” of oral, wire, and electronic communications by anyone, including private individuals, businesses, government entities, government personnel, and law enforcement personnel. Idaho, like a number of other states, has also passed legislation protecting security in oral, wire, and electronic communications. The Idaho Communications Security Act (“I.C.S.A.”), Idaho Code §§ 18-6701-18-6725, which is modeled after the federal Wiretap Act, likewise prohibits anyone from engaging in intentional unauthorized “interception” of oral, wire, and electronic communications.

Under both the federal Wiretap Act and the I.C.S.A., violators are subject to criminal penalties, including fines and imprisonment. Both statutes also provide for a private right of action for those claiming that their oral, wire, or electronic communications have been unlawfully intercepted. Persons who prove their communications have been intercepted in violation of the Wiretap Act and the I.C.S.A. are entitled to recover either compensatory economic damages or statutory damages, punitive damages, attorney fees, and litigation costs.

Under both the federal Wiretap Act and the I.C.S.A., the term, “intercept” is defined as “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” In *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), a landmark decision involving an employee’s right to protection from employer access to his password protected Internet communications, the Ninth Circuit Court of Appeals held that the term “intercept” used in the Wiretap Act means acquisition of a communication which is contemporaneous with its transmission. The classic instance of “interception” under the Wiretap Act is when a person records or listens in to a telephone conversation as the conversation is taking place, without the knowledge or prior permission of either party participating in the conversation. Idaho courts have not yet had the opportunity to interpret and apply the I.C.S.A. in a case involving electronic communications, but, when the time comes, they will be guided by the federal courts’ interpretations of the federal Wiretap Act after which the I.C.S.A. was modeled.

Third parties (including employers) usually do not acquire e-mail and other electronic communications by intercepting the communications during transmission. Instead, third parties typically obtain e-mail messages and other electronic communications from the electronic files in which the communications are stored either prior to, or after, the communications have been transmitted. The Ninth Circuit Court of Appeals has held a third party’s acquisition of an electronic communication is not an “interception” for purposes of the Federal Wiretap Act if the communication is obtained while it is being electronically stored either prior to or after its transmission. Consequently, the Federal Wiretap Act and I.C.S.A. are unlikely to come into play in cases involving acquisition of e-mail communications. You should, however, keep the Federal Wiretap Act and I.C.S.A. in mind if you are implementing procedures to monitor employees’ telephone communications for quality control or other business-related purposes and ensure that you conduct monitoring in compliance with the wiretap legislation.

The legislation which courts have found applies to cases involving employers’ accessing of employees’ e-mail messages and other electronic communications is Title II of the ECPA, 18 U.S.C. §§ 2701-2711, known as the Stored Communications Act. The Stored Communications Act prohibits anyone without authorization from intentionally accessing a facility through which an electronic communication service is provided and thereby “obtaining, altering, or preventing authorized access to” electronic

communications while they are in “electronic storage” in the facility. The ECPA defines “electronic storage” as being any “temporary, intermediate storage” which is “incidental to the electronic transmission” of an electronic communication and as any storage of the communication “by an electronic communication service for purposes of backup protection.”

Federal courts which have interpreted the ECPA’s definitions of “electronic storage” disagree on the scope of the definitions’ applications. But those courts do agree that the Stored Communications Act protects e-mail messages being stored on a server at any point in the transmission process pending delivery. The Ninth Circuit Court of Appeals has found that the Act protects e-mails being maintained in storage by electronic communications service providers, both prior to and after delivery, in order to preserve the e-mails from permanent deletion. Therefore, the Act essentially prohibits persons from gaining unauthorized access to e-mails stored on electronic communication service provider’s servers and doing things like printing, copying, forwarding, or deleting stored e-mails, or changing the account holder’s password so as to prevent her from accessing her e-mails.

Those who violate the Stored Communications Act are subject to criminal penalties, including fines and imprisonment. Like the Federal Wiretap Act and the I.C.S.A., the Stored Communications Act provides for a private right of action for those claiming their stored electronic communications have been unlawfully accessed. Persons who prove their communications have been accessed in violation of the Stored Communications Act are entitled to recover either compensatory economic damages or statutory damages, punitive damages, attorney fees, and litigation costs.

The Stored Communications Act does not apply to an employer who accesses an employee’s electronically stored personal e-mails if the employee has given the employer prior authorization to do so. The Act also makes an exception for those who access stored electronic communications with prior authorization from the provider of the electronic communications service. The term “provider” is not defined by the ECPA, but at least one Ninth Circuit federal court has held an employer was a “provider” of electronic communications services under the Act because the employer provided the computer terminals, software, and equipment which permitted employees to engage in transmitting personal pager messages, which the employer ultimately accessed after the messages had been stored on the employer’s computer system.

Thus, if an employer provides the computer terminals, software, and equipment which facilitates a workplace e-mail or other electronic communication system, Idaho courts will likely follow the lead of federal courts by deeming the employer a “provider” of the communication services under the Stored Communications Act, and by finding the employer is therefore exempt from the Act’s application with respect to accessing employee e-mails which are stored on the employer-provided computer systems. Nevertheless, the best practice for avoiding potential liability under the Act is to obtain your employees’ prior consent and acknowledgement that you reserve the right to control and access all electronic files on your computer systems, including e-mails stored in your systems, regardless of whether your employees have designated those files as “personal.”

Employers are subject to liability, however, under the Stored Communications Act if they directly access employees’ e-mails from personal e-mail accounts, such as Hotmail, which are maintained by remote Web-based electronic communications service providers. Federal courts have found the Act applicable in cases where employers made unauthorized uses of known personal e-mail account passwords, or successfully guessed account passwords, in order to obtain e-mails from their employees’ personal e-mail accounts which were provided by remote electronic communications service providers. So to avoid potential liability under the Stored Communications Act, you should not go into your

employees' personal e-mail accounts, even just for purposes of monitoring their Internet usage, unless you have obtained their prior consent specifically permitting you to access the private accounts.

On the other hand, courts have consistently viewed e-mails which employees download from their personal e-mail accounts and store on their employers' servers as being the same as other electronic files stored on the employers' servers. Therefore, in most circumstances, you will have authority under the employee authorization and/or provider exceptions to the Stored Communications Act to access employees' personal e-mails which they have downloaded from personal e-mail accounts and stored on your servers.

The Federal Wiretap Act and the I.S.C.A. expressly prohibit using communications obtained in violation of those statutes as evidence in court proceedings. The Stored Communications Act does not expressly prohibit using the content of stored electronic communications obtained in violation of the Act as evidence in court proceedings. Both Idaho and federal courts, however, will likely interpret the Stored Communications Act as giving courts discretion to exclude evidence of stored electronic communications which have been obtained in violation of the Act. Furthermore, other federal or state laws, including privacy laws and laws pertaining to attorney-client privilege, may preclude disclosing and using acquired communications as evidence.

For these reasons, in a wrongful termination lawsuit, even incriminating employee communications which are supportive of the employer's basis for termination are subject to being excluded as evidence if such communications were wrongfully obtained in violation of the ECPA or the I.S.C.A. If, however, the e-mails or other electronic communications are relevant to an employee's wrongful termination lawsuit and are not subject to the attorney-client privilege, or protected from disclosure by some other law, you can legitimately obtain the communications from the employee through discovery in the lawsuit, regardless of whether the files had previously been protected under the ECPA or the I.S.C.A.

Claim For Invasion of Personal Privacy

In addition to statutory claims under the ECPA and the I.C.S.A., employees who believe their employer has wrongfully accessed their personal e-mails or other electronic files may bring a tort claim for invasion of privacy. Idaho courts recognize a claim for invasion of personal privacy based on intrusion into a person's private affairs. This claim applies when an employee contends her employer improperly accessed her personal e-mails or other personal electronic files. In order to establish an invasion of privacy claim, an employee is required to prove the following: (1) that she is entitled to privacy in the electronic files at issue; and (2) that the employer's alleged intrusion into her right to privacy was of a type which is offensive to a reasonable person.

Making an invasion of privacy claim is usually an uphill battle for the employee when the e-mails or other electronic files, which she claims her employer wrongfully accessed, are being stored on the employer's computer systems. A factor courts consider especially significant, and which has invariably weighed strongly in employers' favor, is the employee's consent to policies prohibiting personal use of employer-provided computer systems and to employer monitoring of employee computer uses and electronic files. Employee consent to employer monitoring of their computer uses and files nullifies their expectation that they have personal privacy with respect to any files they send or store on their employer's computer systems.

Courts have also recognized employees have a diminished expectation of personal privacy in their activities on employer-provided computer facilities because those computer terminals, software, and systems are controlled by the employer and are provided to employees for work-related uses rather

than for private personal uses. Employee e-mails sent through the employer-provided e-mail system and other electronic files stored on the system belong and are always accessible to the employer; therefore, employees cannot reasonably expect that their electronic files are actually private, even if they designate files as “personal.”

Along the same lines, courts have found that e-mails sent using an employer-provided system are potentially viewable and subject to further dissemination by anyone with access to the e-mail system, including the intended recipient and the employer, and, as such, employees cannot maintain a reasonable expectation of personal privacy in such e-mails, even if they later store the e-mails in a personal password protected file on their employer’s server. Additionally, courts have found the foregoing factors apply to diminish employees’ expectation of personal privacy in e-mails which they download from their personal remote Web-based e-mail accounts, such as Hotmail, and save on their employers’ servers. Once the downloaded e-mail is saved on the employer’s system, the file becomes subject to the employer’s access and control just like any other electronic files in the employer’s computer systems.

Courts, however, have found employees have a higher expectation of personal privacy in e-mails stored in their personal password protected e-mail accounts, such as Hotmail, which are provided by remote Internet service providers, even when the employees have accessed the accounts from their workplace computers. Although the issue of an employee’s right to privacy in personal password protected e-mail accounts has not yet been addressed by either of Idaho’s appellate courts, in light of federal courts’ decisions addressing the issue, an Idaho employer who directly accesses the contents of an employee’s personal remote Web-based e-mail account without the employee’s prior consent runs the risk of liability for invading the employee’s right to privacy.

Employers may protect their legitimate business interests by monitoring the types of employer-provided Internet uses in which their employees are engaging if such monitoring consists only of compiling logs showing the Website addresses visited by employees rather than accessing the content of visited sites. Courts addressing employer monitoring of employee Internet use have found employees do not have an expectation of privacy in Internet use records because that information is readily accessible to the employers who control their own computer systems and, as such, the record of Internet use is not actually private information. Employers’ cases have been further strengthened when their employees were given prior notice that employee Internet uses would be monitored.

Finally, courts generally recognize that employees’ expectations of personal privacy in personal e-mails and other electronic files on their employers’ computer systems may be outweighed by employers’ legitimate business interests in securing proprietary information from unauthorized uses, in maintaining a professional atmosphere, in protecting the employers’ business from liability for unlawful workplace discrimination or harassment, and in protecting business equipment from being used by employees to perpetrate crimes such as obtaining child pornography. When courts find that an employee lacks a reasonable expectation of personal privacy in the e-mails or other electronic files at issue and that the employer has demonstrated a legitimate business reason for accessing those files or for monitoring employee’s Internet uses, courts will likewise find that the employer did not commit an invasion of personal privacy which would be offensive to a reasonable person.

Pointers For Protecting Your Business & Avoiding Employee Claims For Invasion of Privacy

- First and foremost establish clear, concise, and comprehensive policies nullifying employees' right to privacy in electronic communications carried out and stored on the computer systems you provide. Your policies should have three components. First, you should notify your employees that workplace computer equipment and computer systems, including internet access, are provided to them for work-related uses only and that personal uses are prohibited. You should also identify more specifically the types of non-work related uses which are against your policy such as downloading and disseminating materials which are illegal, pornographic, sexually or racially offensive, or harassing. Secondly, you should expressly notify your employees that as the provider of computer equipment and services, you retain the right to control and monitor uses of those facilities and, as such, employees will have no right to privacy in any files sent over your e-mail system or stored in your facilities, regardless of whether such files are designated as "personal" or are saved in personal password protected files. You should further notify your employees that you will routinely monitor the electronic files stored on your computer systems and employee uses of the Internet access you provide. Finally, you should notify your employees that those who violate your computer and Internet use policies will be subject to discipline.
- Have your employees sign a written acknowledgement that they have received, read, and accepted your computer and Internet use policies. The written acknowledgement can be a powerful weapon to defeat an employee's claim that she expected her personal e-mails and electronic files stored on your computer systems or the record of her personal Internet use would be private and protected from your monitoring activities.
- Routinely remind your employees of your computer and Internet use policies by circulating memos re-iterating the policies and by discussing the policies in training sessions and staff meetings.
- Do not go into your employees' personal password protected e-mail accounts, such as Hotmail or Netscape, which are provided by a remote Internet service provider.
- If you believe an employee's personal e-mail communications or other personal electronic files are relevant to litigation between you and the employee, but you are aware that the files might be subject to protections under the ECPA, I.S.C.A., or Idaho law protecting personal privacy rights, protect your ability to use the files as evidence by waiting until you can legitimately obtain them through discovery in the lawsuit.