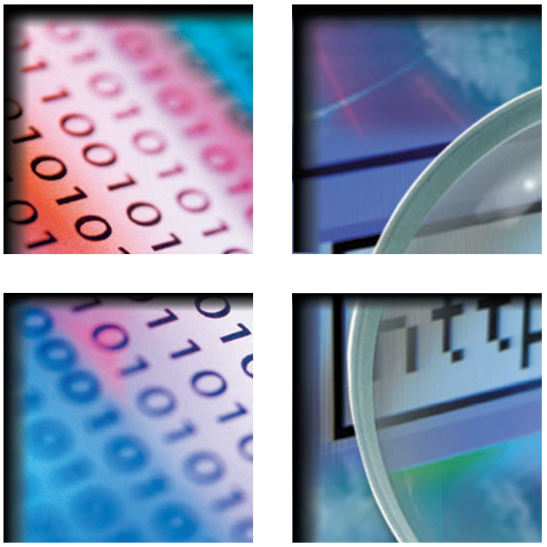
Internet Manager®
Family of IPM Solutions

Employee E-mail and Internet Risks:
Policy Guidelines and Investigations

By Mark E. Schreiber

Labor & Employment Law Department
Palmer & Dodge LLP, Boston



ELRON SOFTWARE

 Earlier versions of this article by this author and Emily C. Ehl appeared in THE JOURNAL OF BIOLAW & BUSINESS [ed: RJRBlatt] Volume 3, Number 1, pp. 19-29 (1999) ‹www.biolawbusiness.com›, and in Pike & Fischer INTERNET LAW AND REGULATION, SPECIAL REPORT (DEC. 1999) ‹http://internetlaw.pf.com›. Reprinted with permission. The author is especially indebted to Emily C. Ehl, an associate in the Labor & Employment Department at Palmer & Dodge LLP, for her work on the privacy sections of this article; to Peter E. Schwartz and Ali Levin, associates, and Matthew J. Zweig and Kathy Cloherty, law student interns, who provided invaluable assistance; to partner Michael Brown and associate Sally Adams for their work on an unpublished monograph, "Privacy Issues in the Employment Context," which helped inspire earlier versions of this article; and to others at the Firm for their helpful comments and assistance.

Table of Contents

Overview

Cyberstalking, on-line threats of violence, sex sites and "spam" complicate the efficiency and compromise the integrity of employer-provided systems and Internet access. Companies may face claims of discrimination or sexual harassment arising from their employees' sexual, racial, or otherwise threatening or harassing e-mails or Internet graphics or messages, as well as for defamation, copyright infringement, fraud or other claims related to employee misconduct. Studies show that upwards of 85% of employees surveyed use e-mail at work for personal purposes, 62% of organizations report employee sex site surfing, and some 55% of employees have received sexual, racial or other inappropriate e-mails during work. [1] As the workplace catches up with technology, employers are increasingly becoming concerned about employee use of computer networks and the Internet for personal e-mail and for a myriad of questionable purposes such as "playing games, downloading pornography, ordering goods online, checking stock prices, or gambling." [2] Companies also are considering the impact that "cyberloafing" has on employee productivity [3] , and the resulting extra demand which that activity and "spam" place on employer systems. [4] Another recent study indicated that approximately 73% of large companies now monitor employee e-mail, computer files or calls, [5] an increase of nearly twofold from 1997.

To deter inappropriate use and to protect themselves better, employers should implement, disseminate, and enforce e-mail and Internet use policies that are tailored to their specific business needs. Such policies should explicitly describe the permitted and prohibited uses of the employer's e-mail and Internet systems, and make clear that employees do not have an expectation of privacy in their e-mail and Internet use. Accordingly, the policy should state the manner in which employees' business and/or personal e-mail or Internet communications can or will be accessed or monitored by the company. New federal legislative proposals would require general notice to employees as a condition of monitoring, [6] which notice in turn would further legitimize employer e-mail oversight. [7]

Employers may need to review employee e-mail or Internet traffic during internal investigations or to prevent employee abuse of its systems. The mechanics of an e-mail review are sometimes demanding, including questions such as who should conduct it, should files first be backed up before being opened or read, which files should be opened and how are they to be identified? An employer who accesses or monitors these systems should do so judiciously, with a legitimate business reason, and employ the least intrusive means to do so. To accomplish these goals, employers need to familiarize themselves with the latest variations of e-mail and Internet filtering software, as well as stay abreast of the developing law in this area.

Whether or when an employer may or should seek redress for an employee's misuse of its e-mail system, or may even be liable for it, are perplexing legal issues that are not yet resolved. In some instances, employees assert that they have a privacy interest in and legal protections from their employer capturing or reading their e-mail messages or Internet traffic but almost all of these claims have proven unsuccessful to date.

Taken together, the burgeoning caselaw and new statutes, regulations and proposals constitute the emerging field of "workplace cybermonitoring," an area of law and technology that scarcely existed several years ago.

I. Employee Misuse of E-mail and the Internet

The informality with which some employees send e-mail messages, or download or electronically pass onto others problematic, inappropriate or offensive materials has significant potential for abuse. Such practices have all ready begun to manifest in litigation. As one experienced trial lawyer put it:

> The most intimate e-mail conversations are filed and retained by machines that don't care how careless we were with our language. When used as evidence, they take on the magic and formality of a real document.[8]

Several recent cases highlight the seemingly endless ways in which employees can expose their employers to potential liability, illustrate the complexities and new challenges facing employers, and provide an indication of precautions companies may want to consider when designing or updating policies.

Employee Chatroom Cases

Defense contractor Raytheon Co. filed suit against twenty-one of its employees for allegedly posting private company information on a web site operated by Yahoo, Inc. The suit was brought after Raytheon discovered that these employees used anonymous screen names to enter a chatroom and discuss private company financial information which activity, according to Raytheon, was detrimental to the company. [9] After the suit generated publicity, Raytheon issued a policy statement regarding employee use of the Internet, which stated that although employees may discuss the company on the Internet, they must not reveal or disseminate company proprietary information. To determine which employees participated in these communications, Raytheon demanded that the relevant Internet Service Providers (ISPs) disclose information they had concerning the identity of the anonymous users. The case was reportedly dismissed voluntarily by Raytheon after the extent of the disclosures was limited and some employees resigned.

A similar case filed by Dyna Gen, Inc. against two former executives for false and misleading statements allegedly made in an Internet chatroom was also reported. [10]

Emulex, PairGain and Other Stock Manipulation Cases

There are an increasing number of stock fraud and price manipulation cases occurring on the Internet. The FBI arrested a former employee of Internet Wire, Inc., a web news service, for allegedly creating a false press release which drove Emulex stock down by some 50% before the hoax was discovered. The bogus release, picked up by other news services, said that Emulex was restating its earnings, was the subject of an SEC investigation and that its CEO had resigned. [11] With the sudden price drop, the ex-employee allegedly garnered nearly $250,000, making up for his prior stock losses. Emulex's market capitalization dropped $2.5 billion prior to recovering.

An employee of PairGain Technologies Inc., a maker of telecommunications software, also posted a false report on the Internet, stating that it was going to be acquired by an Israeli company. [12] As a result, the value of PairGain stock rose approximately 32% before the fraud was discovered. The employee used a pseudonym and replicated the logo of a brokerage firm to post the report on a message board that did not require identification. The FBI traced the message to computers allegedly used by the PairGain employee. The FBI investigation included subpoenaing records of Microsoft's free HotMail service and examining PairGain's computer logs to trace the employee's Internet use on his work computer. The employee was charged with a scheme to defraud investors and he later reportedly pled guilty.

The SEC announced guilty pleas of two men in California for stock price manipulation and false statements over the Internet where the defendants wrongly claimed that NEI Webword, Inc. and other online entities would be acquired. [13] They were charged with civil and criminal violations, including conspiracy to commit securities fraud. Together the defendants allegedly made nearly $700,000 in illicit profits, which the government sought to recover and whose assets the court froze. [14]

Sexual and Racial Harassment

With increasing frequency, inappropriate or offensive e-mails and web communications are surfacing in race and sexual harassment suits. Three major U.S. corporations— R.R. Donnelley & Sons Co., Morgan Stanley & Co. and Citicorp's Citibank N.A.—were sued by black employees for racial discrimination as a result of e-mail messages containing allegedly racist jokes. [15] In Harley v. McCoach, [16] a Pennsylvania employer faced a claim of racial harassment that involved an e-mail identifying the plaintiff as "Brown Sugar." Plaintiff's allegations were insufficient to support a hostile work environment claim. [17] In Copley v. Bax Global, Inc., [18] a race discrimination case, the court held that the employer's e-mail messages discussing logistics of plaintiff's termination were "highly probative circumstantial evidence" of the employer's discriminatory motive and denied the employer's motion for summary judgment.

Employees' sexual e-mail messages or graphics are now commonplace in sexual harassment cases. In Schwenn v. Anheuser-Busch, Inc., [19] an employee sued her employer for sex discrimination, claiming that she had received sexually harassing e-mail messages from her co-workers. Likewise, in Rudas v. Nationwide Mutual Ins. Co., [20] an employee sued her company for retaliation after she complained that her supervisor sexually harassed her by sending her explicit e-mails. While the courts in both cases granted summary judgment for the employer, cases involving more frequent or pervasive sexual e-mails may survive summary judgment. For example, in Knox v. Indiana, [21] a suit brought by a female correction officer was allowed to go to trial based in part on e-mails the plaintiff had received from her supervisor asking her for sex. The emails often involved acronyms, such as asking the plaintiff "whether she wanted to have a HGTWM," which was later translated as a "horizontal good time with me." [22] The jury, however, ultimately found against the plaintiff on her claims.

Under both state and federal anti-discrimination laws, employers have the obligation to undertake prompt remedial action if sexual harassment is found. Curtailing offensive e-mail or imported or exported web traffic or graphics is no exception. [23] One state agency, the Massachusetts Commission Against Discrimination (MCAD), is in the process, in collaboration with the private bar, of compiling guidelines for investigation of sexual harassment complaints. A draft portion addresses employee e-mail and Internet use, treats these the same way as other evidence, and suggests employer oversight to prevent or remediate harassing e-mail messages or material.

Defamation

Employers may also have to defend against defamatory e-mail communications. In Meloff v. New York Life Ins. Co., [24] a discharged employee brought an employment discrimination and defamation claim against her former employer because of an e-mail sent to others at the company improperly stating that the reason for her termination was credit card fraud. In Lian v. Sedgwick James of New York, Inc., [25] the plaintiff's unsuccessful defamation claim was based on his former supervisor's e-mail to other employees, which stated that plaintiff had agreed to seek other employment and would not transact further business on behalf of the company. In an electronic "bulletin board" case, Blakey v. Continental Airlines, Inc., [26] the New Jersey Supreme Court sent a defamation and retaliation case back to the trial

court to determine whether the employee-run Crew Members Forum was "sufficiently integrated" into the workplace to require employer intervention and/or impose employer liability for alleged defamatory postings.

Under federal law, an employer is not liable for defamation due to Internet communications unless the employee acts within the scope of his employment and the employer either had knowledge of, ratified, or recklessly disregarded such conduct. [27] There is also qualified immunity for liability where the company is a service provider. [28]

Employers must also take care in accusing employees of improper Internet usage. In an ironic twist in Barker v. Kimberly-Clark Corp., [29] an employee sued her employer for slander when her supervisor accused her of accessing Internet pornography on a company's computer. The supervisor became aware of the alleged improper use from another employee's accusations, but did not investigate further. The plaintiff alleged that the supervisor's accusations were made in front of third persons, and impugned her reputation in her trade or business. The Court of Appeals of North Carolina reversed the trial court's entry of summary judgment for the defendant employer, holding that the supervisor made the statements with "reckless disregard for the truth," and thus a triable issue of fact existed regarding her slander claim.

Copyright Infringement

Employers can face liability for copyright infringement where an employee improperly places copyrighted materials on the Internet. In Marobie-FL, Inc. v. Nat. Ass'n of Fire Equip. Dist., [30] a software company successfully brought a claim against the association for copyright infringement after an employee placed files containing copyrighted clip art on the association's web page. There are also several new computer-related federal crimes designed to protect intellectual property rights and trade secrets, including amendments to the Copyright Infringement Act, the Computer Fraud and Abuse Act, and enactment of the Economic Espionage Act of 1996. [31]

Union Issues

In unionized environments, employers have to address claims by unions seeking to contact employees through the company e-mail system or other interference or retaliation claims. If access is denied, claims of anti-union discrimination may be asserted. In the latest case, Adtranz, ABB Daimler-Benz Transportation, N.A., Inc., [32] the NLRB affirmed an administrative law judge's finding that the employer's e-mail policy, which prohibited non-business e-mail use, was facially valid and fairly applied. The ALJ had rejected the contention that the e-mail policy unlawfully interfered with union employees rights under Section 7 of the National Labor Relations Act (NLRA). The judge reasoned that since previous NLRB decisions held that unions do not have a statutory right to use bulletin boards and telephones for non-business purposes, they should not have the right to so use the employer's e-mail system. Critical to the ruling was the fact that the employer did not apply the policy in a discriminatory manner. While the employer did allow personal e-mails, there was no evidence that it attempted to exclude the union as a topic for discussion.

The NLRB General Counsel in an Advice Memo has been particularly aggressive in asserting that a company policy prohibiting all non-business e-mail was overbroad and unlawful, especially where employees regularly sent personal e-mail at work. [33] Earlier, in E.I. du Pont de Nemours & Co., [34] the NLRB ruled that the company's e-mail policy which allowed the e-mail system to be used for non-business communications but not for the distribution of union literature, was discriminatory and violated Section 8(a)(1)

of the NLRA. Similarly, in Timekeeping Systems Inc. v. Leinweber, [35] the NLRB held that a company violated the NLRA when it fired an employee for sending an e-mail message criticizing the company's vacation policy to other employees. The NLRB ruled that the employee's e-mail communication was protected concerted activity and that it was unlawful for the company to terminate the employee for this reason. These cases suggest heightened NLRB scrutiny of whether a computer network is a "work area." [36] Other issues such as an employer accessing a union website may also be raised.

Negative Publicity

In addition to exposing employers to liability, employee misuse of employer systems can lead to unfavorable publicity. In the spring of 1999, the dean of the Harvard Divinity School resigned, reportedly "for conduct unbecoming a dean," after the school discovered that he stored quantities of alleged pornographic material on his Harvard-owned computer. [37] Sources at the School said they were concerned that the scandal would damage the Divinity School's reputation. [38]

II. Drafting Workplace E-mail and Internet Policies

Employers should provide employees with a clear policy statement describing the permitted and prohibited uses of employer e-mail and Internet systems, which include statements that e-mail and Internet messages and traffic on company systems are not the private property of employees and that the employer has the right to — and will — monitor employee e-mail and Internet use. There are many reasons for such a policy, among which are: 1) to set boundaries for appropriate employee conduct; 2) to dispel employee expectations of privacy; and 3) to foster employee consent, either direct or implied. A clear policy helps reduce legal exposure and bolster employer defenses to employee claims, including for invasion of privacy. [39]

Subject to the company's specific practices, such a policy should include statements that:

- the Company's e-mail and Internet systems will be used and its policy implemented in a manner consistent with its other policies, such as those prohibiting sexual harassment;
- the system is solely for business use, and personal use is prohibited; or
- the system is primarily for business use, but limited personal use is permitted, as long as it is not excessive and does not interfere with business needs or operations;
- the e-mail and Internet access systems and hardware are the property of the company, and all pass codes and all e-mail and Internet messages and attachments composed, sent, or received are the property of the company;
- employees should not consider information on the system private, including e-mail messages, content, attachments and web sites visited;
- incoming and outgoing messages and attachments are subject to being accessed, reviewed, disclosed or monitored – and will be monitored – at the sole discretion of the company, in the ordinary course of its business, at any time, with or without notice, and notwithstanding any password;
- the employer has the capability and reserves the right to – and will – track and monitor employee use of the Internet, including web sites visited and files downloaded by the employee;
- the electronic mail and Internet systems are not to be used to create any offensive or disruptive messages. Among those which are considered offensive are messages or material which contain sexual implications, racial or ethnic slurs, or other comments that offensively address someone's age, sex,

sexual orientation, religion, national origin, ancestry or disability. In addition, the system must not be used to communicate other improper messages, for example, messages or material that is defamatory, derogatory, obscene, or otherwise inappropriate;

- the electronic mail and Internet systems must not be used to commit any crime, including but not limited to sending obscene e-mails over the Internet with the intent to annoy, abuse, threaten, or harass another person;
- employees must not visit sexually explicit, offensive or otherwise inappropriate Web sites or engage in computer games or gambling activities;
- the system must not be used to violate any law, regulation, or company policy;
- the system must not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior management authorization;
- employees must not create, send, or forward "chain letter" e-mails or engage in "spam;"
- employees must not use the system to solicit for personal business endeavors or undertakings that are not job related, or assist others in doing so;
- employees must not access other employees' e-mail without prior management authorization;
- the mere deletion of a message or file may not eliminate it from the system;
- no former employee may access or use the systems, without authorization.
- employees who need help understanding this policy or who discover a violation of this policy should notify [the employer's designee]; and
- a violation of the policy may result in disciplinary action ranging from a verbal warning or suspension of system privileges up to discharge from employment.

Some companies add voicemail to the systems covered in these policies. In addition, employers, depending on their type of business, goals and corporate culture, may want to consider including some of the following provisions: [40]

- employee e-mail will be treated consistently with the company's document retention policy;
- employee passwords are confidential, and employees are accountable for all usage under their password of the company's computer system;
- employees with Internet access must take particular care to comply with and understand the copyright, trademark, libel, slander, and public speech control laws of those countries in which this company maintains a business presence;
- confidential or privileged information should not be sent over the Internet, unless with appropriate warnings, safeguards, or encryption;
- only company approved encryption methods may be used and then only by authorized employees;
- employees should make clear when they are or are not representing the company in their e-mail or Internet communications;
- employees [may/may not] engage in chat, chatroom or bulletin board activities;
- executable files may not be downloaded without prior authorization;
- employees should not open e-mail or attachments unless they are confident of the identity of the sender.

Massachusetts public or governmental employers have special obligations and their e-mail and Internet policies require additional provisions addressing e-mail retention and disclosure as public records and applicability of the Open Meeting Law.

The employer's e-mail and Internet use policy should be distributed to all employees and posted in a prominent place. Additionally, employers often have employees sign a standard acknowledgment that they have received and read the policy, do not have an expectation of privacy, and that they understand that the employer may monitor their e-mail and Internet use. Other employers have "pop-up" messages prior to initial e-mail or Internet log-on stating that "logging on" or use of the system constitutes express consent to the employer's policy, including monitoring. Finally, employers should enforce their policy in a uniform manner.

Unfortunately, employers sometimes find themselves in the midst of a serious problem or internal investigation before adopting an e-mail policy. An employer should try not to put itself in the position of having no policy or an ambiguous policy and then address whether it can or should examine e-mail messages during an internal sexual harassment or fraud investigation. To avoid such situations, companies should be proactive in the development of their e-mail and Internet use and monitoring policies, anticipating these possible dilemmas. Absence of a policy will not, however, eliminate a duty to investigate employee e-mail or Internet misconduct.

Human resources and management information services departments of the company will need to cooperate in the development, execution and oversight of e-mail and/or Internet technology policies. The input of both departments should be sought to maximize personnel and technology expertise, consistent with the employer's norms.

Company Dilemmas In Enforcement

Dilemmas may arise when determining corporate policy choices and enforcement practices. One major issue is finding the balance between appropriate controls and what some may perceive as draconian measures. Other questions that need to be considered include:

1. Will such policies create employee resentment and/or erosion of trust in the employer?
2. Should some private use be permitted at work? If so, how much or how should it be monitored?
3. Does permission for limited private use create an expectation of privacy, and how should this be curtailed?
4. What about off-site, remote access, after-work hours use on a company system or personal web sites?
5. What discipline should be exercised, and in what instances, for violation of the policy?
6. How is the gravity of the workplace offense to be evaluated?

The answers to these questions need to be tailored to the employer's norms and the company's particular culture. In certain workplaces, particularly biotechnology or high tech, personal use of e-mail and the web are commonplace, if not expected. As such, employers in these environments may be concerned that a "no personal use" policy would dissuade new hires or cause disaffection among present employees.

On the other hand, more highly regulated employers, such as in financial services, brokerage houses or banks, understandably may be more restrictive and opt for closer monitoring and more severe sanctions. For instance, one brokerage firm, Edward Jones & Co., announced that it fired nineteen employees because of the employees' failure to admit that they sent inappropriate jokes or pornography over

the firm's e-mail, while giving written warnings to forty-one workers who voluntarily acknowledged e-mail abuse. [41] Strict enforcement policies are not limited to the financial sector, however. The New York Times Co. reportedly fired more than twenty employees in its Norfolk, Va. payroll processing center for sending e-mail that was "inappropriate and offensive." [42] Xerox Corp. also made headlines by firing forty workers for viewing pornographic web sites at work.[43]

Employer Use of E-Mail and Web Filtering Software

Once a decision is made to pursue e-mail or Internet oversight, follow-up discussion on policy implementation, including the possibility of filtering software, needs to be addressed. Elron Software, an advanced filtering software provider, suggests that management first address these basic questions:[44]

1. Who in the organization needs Internet access? Which individuals? What business areas? What functional areas?
2. What Internet services does the user need? E-mail? File Transfer? World Wide Web Browsing? Remote access to customers, suppliers, sites, data vendors or research services?
3. What kind of access does the user need? Full-time, periodic, or casual?
4. Will the user need Internet access to be integrated into productivity-type activities like word processing? Will a core business application have to be Internet-enabled?

Some employers can adequately utilize in-house capacity to perform these monitoring and filtering tasks. If not, there is both e-mail and web filtering software technology commercially available. One e-mail filtering approach is based on a list of blocked terms, using what is called "key word" or "string match" technology, such as ["sex" and "girl"]. Unfortunately, these methods are reported to create a large number of false hits or false positives. Management can obtain more accurate results when a system not only blocks terms where appropriate, but also contains a lexical analysis which checks the context of the message. Other new products use complex algorithms to detect signs of improper use, with patterns displayed in three dimensional graphics to examine relationships.

The common approach to web filtering is to rent a "block list." Issues with this approach include, for example, who determines the sites to be blocked? How often will the company have to update these lists? How many sites are to be added to these lists daily? How much storage space do these lists require?

Another Internet filtering approach is a technology that automatically builds and maintains a list of restricted web sites without the need for continuous third party updates. With this approach, network managers can set their own criteria for blocking web sites by creating a "Suspect Dictionary" containing key words. Whenever a user attempts to access a site containing one of the keywords specified in the "Suspect Dictionary," the filtering solution will automatically block access to the suspect site and add the web site address to its list of restricted sites. This technology can also automatically verify the "suspect" site based on the actual text on the web page, in addition to the name or URL "header." New software programs give an employer the ability to automatically forward offensive e-mails to an administrator or department manager and/or to send warnings to employees that they have violated company policy. Other programs are being developed to exclude certain categories of messages from employer oversight, for instance allowing employees to e-mail identified family members without being monitored. Yet other anticipated products include selective "spam" blockers which allow in narrow categories of messages and prevent other unsolicited ones. Doubtlessly, there will be developments in future filtering software and increasingly sophisticated personnel to manage these functions.

E-Mail Record Retention Policies and Electronic Discovery

Many companies will want to consider reviewing their document retention policies to integrate and include e-mail and mechanisms for e-mail segregation and retention. Whether or to what extent e-mail may be considered a "personnel record" subject to state or federal laws requiring record retention also remains to be seen. [45] The new federal Digital Signature law, [46] signed June 30, 2000, not only permits electronic signatures, but expands adequate record keeping to include electronic storage for records relating to or affecting interstate or foreign commerce.

Some employers have limited record retention needs and believe that comprehensive e-mail deletion outweighs the risk of deletion of potentially discoverable material. There are now mechanisms that sophisticated employers are reportedly using, occasionally called "data scrubbers" or "housecleaning" programs, that can periodically and permanently erase e-mail, including from the hard drive, area network, and backup tapes. The latest version of certain e-mail packages contain such capabilities. Employers who want to consider implementing such mechanisms should discuss the mechanics of this with their MIS department and counsel. For more regulated industries, this is not an option. [47]

Additionally, once a company is on notice that a claim or litigation has begun, it may have obligations to preserve and not to destroy potentially relevant evidence, including e-mail on backup tapes. [48] In one Massachusetts case on "spoliation" of e-mail evidence, the court assessed penalties, including attorneys' fees and instructed the jury that the company, which did not suspend customary recycling of backup tapes, did so "out of a realization that the evidence was unfavorable." [49] In addition, in Procter & Gamble v. Haugen, [50] a defendant moved for sanctions against Procter & Gamble alleging that the company did not preserve corporate e-mail communications during the pendency of the litigation. Although Procter & Gamble argued that they were not on notice that their e-mail would be relevant, the court imposed $10,000 in sanctions. [51]

Which party should bear the expense of e-mail retrieval in discovery is a hotly contested issue. A Massachusetts court recently agreed that a defendant company must bear the cost of producing computer information. The court pointed out that "[t]o permit a corporation…to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results." [52] In another case, In re: Brand Name Prescription Drugs Antitrust Litig., [53] the court also decided that the defendant should shoulder the estimated $50,000 to $70,000 costs, noting that "the costliness of the discovery procedure involved is…a product of the defendant's record-keeping scheme over which the [plaintiffs have] no control." However, in O'Meara v. Internal Revenue Service, [54] the court refused to impose the cost of retrieving information on a government agency, holding that "[p]laintiff cannot require his fellow taxpayers to assume the expense of his search for information."

III. Effect of E-mail and Internet Policies and Monitoring on Employees' Right to Privacy

Core Considerations

A basic issue in employee rights cases is whether employees have a right to privacy in their e-mail messages. As with most invasion of privacy cases, the core issue is whether an employee had a reasonable expectation that his or her personal e-mail messages or web traffic would be private from his employer (and in the case of a public employer, whether the workplace search is sufficiently tailored under the fourth amendment to the government's interest in the efficient and proper operation of the job site). As

the few reported cases indicate, employees have had little success in suing their employers for invasion of privacy when their employers accessed their e-mails or Internet activity, especially where the company had a clear and well-disseminated e-mail and Internet policy in place.

An argument may be made by an employee that an e-mail message is similar to a letter—it is addressed, written and sent—and thus reading an e-mail message is like opening a letter without permission. On the other hand, one can assert that e-mail is not sealed or sent in a government-regulated environment like the U.S. Postal Service, and thus it is more like to an inter-office memo. As an employer is free to read inter-office memoranda, so too, it is free to read employees' e-mail, the argument goes.

Another issue is the context in which the employee's use of the Internet arises. As one commentator put it:

> But what about the worker who comes to work after having been to the doctor's and been told she has breast cancer? Or the employee who is coming to grips with being a survivor of incest? In both cases, it is probable that they would do some research on the Internet, and just as probable that they would not want anyone— especially supervisors—to know about it. [55]

Invasion of Privacy Claims Generally

Many states recognize a common law right to privacy. Additionally, some states, such as Massachusetts [56] and Rhode Island, have a broad statutory right to privacy while others, such as New York and Virginia, accord more limited statutory privacy rights. [57] While there are different types of privacy claims, the one usually relied on by employees is a claim of "Intrusion Upon Seclusion," [58] which can be explained generally as an unreasonable or wrongful intrusion into another person's private activities or affairs. Generally, an individual bringing this type of invasion of privacy claim must prove that: (1) the defendant intentionally intruded, physically or otherwise, upon the plaintiff's solitude, seclusion, private affairs or concerns; and (2) the defendant's intrusion would be highly offensive to a reasonable person. [59] The precise elements for establishing an invasion of privacy claim based upon intrusion upon another's seclusion, however, vary from state to state.

Recent Case Law

Do employees even have a right to privacy in their e-mail messages and/or Internet use? The presence or absence of e-mail and Internet policies has significantly influenced the courts in their determination whether an employee had a protectable expectation of privacy. These cases underscore the value of an employer having such a policy.

Also, an employee's consent may give rise to a defense to these claims. Most courts hold that if an employee consents to a certain type of activity, then such consent is a defense to a subsequent claim for invasion of privacy. [60] For example, one federal court held that an employer was entitled to summary judgment on former employees' claims for invasion of privacy where the employees understood from the beginning of their employment that they were required to take periodic polygraph tests as a condition of employment and at the time they were given the polygraph tests, they signed releases and authorizations voluntarily consenting to the tests. [61] The same reasoning may be applied in the e-mail and Internet context where the employer provides a policy and/or where the employee signs an acknowledgement or consent form.

No Company Policy—Invasion of Privacy Claim Allowed to Go to Trial

In Restuccia v. Burk Technology, [62] two employees were discharged after the company president, without

prior warning, read their e-mail messages that included nicknames for the president and references to his alleged extramarital affair with another company employee. The Massachusetts Superior Court's summary judgment decision in Restuccia clearly hinged on the employer's lack of an e-mail policy informing employees that their e-mail messages—whether personal or company-related—were subject to scrutiny. The company had no policy against using the e-mail system for personal messages, other than a broad policy against "excessive chatting" on the system, and the employees were not specifically told that supervisors had access to their systems.

Plaintiffs alleged, among other claims, that their termination violated the Massachusetts statutory right of privacy. [63] The court partially denied the company's summary judgment motion and allowed the invasion of privacy claim to go forward to trial. The court stated there was a question as to "whether plaintiffs had a reasonable expectation of privacy in their e-mail messages and whether [the president's] reading of their e-mail messages constituted an unreasonable, substantial or serious interference with plaintiffs' privacy," [64] i.e., whether the company's e-mail search exceeded its legitimate business interests.

The plaintiffs claimed that they did not know that "deleted" e-mails were saved on the company's back-up file and tried to convince the jury that they had a privacy interest in their e-mail messages because they used a password to "log on" to the company network to access the e-mail program. The company offered into evidence the plaintiff's resumes, which indicated that the plaintiffs held themselves out as "computer experts." [65] After a two week trial and three days of deliberations, the jury returned a verdict for the company. [66]

Company Policy—Right to Monitor Upheld

Courts have rejected employees' privacy claims where the employers had an effective e-mail and Internet policy in place.

The California Court of Appeals affirmed an employer's right to access employees' e-mail where the employer had an e-mail policy. In Bourke v. Nissan Motor Corp., [67] the company issued written warnings to two employees after it was discovered that they had sent sexual e-mail messages. After protesting the company's conduct, one employee resigned and the other employee was later terminated. The plaintiffs sued Nissan for invasion of privacy, violation of their constitutional right to privacy, violation of state criminal statutes covering wiretapping and eavesdropping, and wrongful discharge in violation of public policy. Although the plaintiffs argued that they had a reasonable expectation of privacy because they were given passwords to access the system and were told to safeguard the passwords, the lower court granted summary judgment to the employer. The appellate court affirmed, holding that the employees had no objectively reasonable expectation of privacy because the workers had signed a waiver form, stating company policy of restricting use of e-mail to business purposes, and they were aware that co-workers could read their e-mail messages. The court also concluded that the company's conduct was not covered by the state wiretapping statute because it had a right, as the system operator, to access the network.

Similarly, in United States v. Simons, [68] a criminal case in which the defendant was charged with receiving and possessing child pornography, the Fourth Circuit affirmed the lower court's decision that a government employee had no reasonable expectation of privacy in his use of the Internet at work, where the employer had a policy which notified him of Internet audits. The governmental bureau for which the defendant worked had an official policy on Internet use which set out the permitted and prohibited uses of the Internet. [69] The court gave significant weight to the section of the Internet policy pertaining

to audits of employee Internet use, which provided that "audits shall be implemented to support identification, termination and prosecution of unauthorized activity," and could record web sites visited by employees.

No Company Policy—Right to Monitor Upheld

Even in absence of an e-mail policy, however, some courts have held that an employer did not violate an employee's right of privacy by intercepting his or her e-mail. In Smyth v. Pillsbury Company, [70] the court dismissed a claim by a former employee that his former employer had violated his right of privacy by intercepting his e-mail communications and discharging him based upon statements made in those communications. The company repeatedly assured its employees that all e-mail communications would remain confidential and privileged and that the e-mail communications would not be intercepted and used against employees as grounds for termination. Despite these assurances, the company intercepted the plaintiff's e-mail after learning that the plaintiff had sent e-mails to his supervisor concerning sales management that contained threats to "kill the backstabbing bastards" and referred to the planned Christmas holiday party as the "Jim Jones Koolaid Affair."

In rejecting the plaintiff's claim that he had a reasonable expectation of privacy and that the company breached that expectation, the Court stated:

(E)ven if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the company's interception of these communications to be a substantial and highly offensive invasion of his privacy . . . [B]y intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments. [71]

At least one other court has denied an employee's claim for invasion of privacy where the employee was allowed to protect personal e-mail folders with a password. In McLaren v. Microsoft Corporation, [72] the employee asserted that his employer violated his right to privacy by "breaking into" personal e-mail folders and then publishing information to third parties. In dismissing his claim, the court relied on the employer's ownership of the computer and the fact that the e-mail messages were not his property, "but were merely an inherent part of the office environment." The employee was aware that the employer could decrypt the personal password and access the folders, which "were first transmitted over the network and were at some point accessible by a third party." [73]

IV. Statutory Law Affecting Monitoring Employee E-mail and Internet Use

New State Laws and Regulations

Some states have passed laws that specifically address electronic communication harassment or e-mail and Internet monitoring, and employers operating in other states need to be cognizant of them. Alabama, Connecticut, Delaware, Indiana and New York each now have electronic harassment criminal statutes. [74] Both Florida and Maryland require that all parties to an electronic communication consent

before surveillance is lawful. [75] Any person who intentionally intercepts electronic communications without the consent of the parties in those two states may be guilty of a felony. [76]

Colorado and Wisconsin have passed e-mail laws limited to state employers. In Colorado, all public agencies must adopt written e-mail monitoring policies. [77] In Wisconsin, which does not limit e-mail monitoring itself, the ability of state agencies to discipline workers based on information gathered through monitoring is restricted. [78] Wisconsin agencies may only take disciplinary action against a state employee if surveillance produces evidence that the employee has committed a crime. Massachusetts has no such statute but the legislature has had before it a bill aimed specifically at regulating electronic monitoring in the workplace, and there are now House proposals aimed at e-mail "stalkers."[79]

Massachusetts has recently promulgated an executive order requiring that each state office within its Executive Department develop and post a policy regarding "employee expectations of [computer use] privacy." [80] In addition, the Secretary of the Commonwealth announced that e-mails created or received by governmental employees are public records [81] and as such are subject to the requirements of the Public Records Law [82] and public access. However, like all public records, governmental employees' e-mails may be exempt from public disclosure depending upon the content of the e-mails and whether they fall into exempt categories. [83] The Commonwealth's Executive Office for Administration and Finance also advised state agencies to exercise supervision over the use of computer and e-mail resources by its employees, and to retain the right to routinely monitor or inspect network traffic or data. [84]

State Wiretap Laws

In addition to common law or statutory rights to privacy, some states have "wiretap" laws that employees have asserted, albeit unsuccessfully, as a basis for civil claims related to employer e-mail access or monitoring.

In Restuccia v. Burk Technology, [85] discussed above, the plaintiffs also claimed that the defendants unlawfully intercepted their wire communications in violation of the Massachusetts wiretap statute, [86] which prohibits the secret overhearing or recording of wire communications by means of an intercepting device. Defendants successfully asserted on summary judgment that the president's interception of the e-mails came within one of the enumerated exemptions, which provides that: "It shall not be a violation of this section … for persons to possess an office intercommunications system which is used in the ordinary course of their business or to use such office intercommunication system in the ordinary course of their business." [88] The court held that the company's automatic storage of files in a system was protected by the "ordinary course of business" exemption because the employer had a clear business interest in storing computer information on backup files. The court also stated that the alleged "interception" related to backing up files and that the president's subsequent reading of those back-up files was not an "interception" within the meaning of the statute.

The Appeals Court went one step further in Dillon v. Massachusetts Bay Transportation Authority [89] and held that technological advances and "sweeping changes in the telecommunications industry" should, by implication, be read into the Massachusetts wiretap statute "to preserve the substance of a statute rather than diminish it." [90] This expansive reading allowed non-telephone company recording software and devices to fall within the "telephone … equipment" exception to the Massachusetts wiretap statute. In that case, the MBTA was held not to have violated the wiretap statute by secretly intercepting and monitoring employee calls using recording systems of three different commercial makes, which

were not from common carriers and were wired into MBTA operational centers. [91] One can expect further interpretations of this state's wiretap statute to exclude from liability employer e-mail or Internet monitoring efforts, provided such systems have a demonstrable business purpose.

In Flanagan v. Epson America, Inc., [92] employees also failed in a class action against their employer for allegedly violating the California wiretap statute. [93] The employees were required to use a password and asserted that the company illegally "tapped" the e-mail gateway where the mainframe computer interfaced with the outside e-mail communications service and that the defendant "was systematically printing up and reading all of the e-mail that was entering and leaving [the company's facility]." [94] The court found that the wire-tap statute did not apply to the e-mail communications system used by the defendant employer and dismissed the claim.

Likewise, in Bourke v. Nissan Motor Corp., [95] discussed above, another California court held that the California wiretap statute [96] did not apply to an employer's reading of employee e-mail messages. The plaintiffs argued that this statute covered "the retrieval, printing and reading of e-mail messages which [was] not authorized by the author of the message." [97] The court concluded that the company's conduct was not covered by the state wiretapping statute because the company: (1) did not "tap" its own telephone lines; (2) had a right, as the system owner and operator, to access the network; and (3) did not access the e-mail messages during transmission.

Federal Law: Electronic Communications Privacy Act

If the communication system affects interstate commerce, Title I and II of the Electronic Communications Privacy Act of 1986 (ECPA), [98] which amended the Federal Wiretap Act, may apply. The old Federal Wiretap Act has been described as "famous (if not infamous) for its lack of clarity." [99] The ECPA is no better written and is already outdated. Title I prohibits the unauthorized interception and/or disclosure of wire, oral, or electronic communications, while Title II, called the Stored Communications Act, deals with the unlawful accessing and disclosure of communications in electronic storage. The ECPA definitions and other terms were drafted before employer provision of e-mail and Internet systems became standard fixtures in corporate America, and their application to current e-mail and web technology is convoluted at best. Significant proposed amendments to the ECPA have recently been introduced in Congress and the Senate. [100]

The ECPA is usually not an obstacle for employers, as Title I is subject to several exceptions and defenses: 1) communications made with the prior consent of one of the parties to the communication; [101] 2) interceptions by the service provider in the ordinary course of its business; [102] and 3) interceptions by employees engaged in activities incident to provider services or for protection of the provider's "rights or property." [103] Employers will assert that monitoring for employee abuse or misuse of its systems constitutes necessary protection of the company's "rights and property." These exceptions often present a significant if not overwhelming impediment to employees suing under this statute. According to one commentator, "[t]aken together, these exceptions render Title I of the ECPA virtually useless to employees disgruntled over an employer's e-mail monitoring, save for extreme circumstances." [104]

Ironically, in one of the few successful cases under the ECPA, an employer obtained a $42,000 judgment in counterclaim against a former employee for unauthorized access to the company's voicemail system, improper post-employment taping and disclosure of voicemail messages of others. [105] Assertion of or reference to federal statutes like these also subject plaintiff claims in state court to removal by defendant employers to the federal courts, where summary judgment chances on the entire complaint are often better for employers.

Title I of ECPA

Title I of the ECPA primarily prohibits three types of activities: (1) intercepting or endeavoring to intercept electronic communications; [106] (2) disclosing or endeavoring to disclose intercepted information; [107] and (3) using the contents of intercepted information. [108] In addition to criminal sanctions, a civil claim for unlawful interception, as defined, can be brought for statutory and punitive damages, attorneys' fees and litigation costs. [109]

"Contemporaneous" Interception

Numerous courts have held that the intercepting conduct must be "contemporaneous" with the sending of the communication itself for it to be prohibited by Title I. [110] E-mail retrieval and blocking of Internet sites access would not, it appears, be deemed "contemporaneous" or an "interception" under this definition. For instance, retrieval from electronic storage, hard drive or back-up tapes subsequent to actual transmission does not fall under Title I. [111] Such acts may be encompassed under Title II, which has somewhat more helpful language for employers. Also, because interception under Title I is defined as the "acquisition of the contents" of any electronic communication, [112] an Internet screening device or software which blocks employee access by designated domain names, URL's or sites (and does not access content) would probably not fall within the prohibitions of Title I. In fact, screening pornographic or other offensive Internet sites is encouraged under another federal statute, the Communications Decency Act (CDA), discussed later. [113]

Consent Defense

As long as the monitoring employer is not acting for a tortious or criminal purpose, an electronic communication can be intercepted by a party to the communication or where one of the parties to the communication gives prior consent to the interception. [114] As an example, in S.L. v. Friends Central School, [115] a Federal District Court held that the ECPA had not been violated where one of the parties to a "conversation" on AOL instant messenger had effectively consented to the "interception" of the communication by printing it out. Thus, even if some monitoring activity could be viewed as "contemporaneous" or an "interception", to the extent that employees provide their employers with prior consent to monitor their e-mail, such conduct is likely to be excepted from the ECPA.

To protect itself under the consent exception, an employer should publish an unambiguous monitoring policy to its employees and, if practicable, obtain the written acknowledgment or consent of employees. Many companies opt not to have written employee sign-offs or "pop up" boxes for initial employee log-on. These employers can still assert or buttress the argument that an employee has given implied consent by an awareness of the policy and subsequent use of the employer's electronic communications system.

What constitutes "prior consent" is not necessarily a simple question and, especially in the case of implied consent, is likely to turn on the specific facts of a given case. [116] Consent is not defined in the statute and there are virtually no cases involving monitoring of e-mail or Internet activities in which the term has been discussed under the ECPA. One court, in interpreting disclosure issues under the ECPA, noted that service provider agreements with the subscriber nullified any privacy interest of the individual.[117] An analogy can also be drawn from those cases involving telephonic or other non-electronic communications in which the consent exception was raised. In one case, Griggs-Ryan v. Smith, [118] the landlady who tapped her tenant's phone calls was successfully able to rely on the consent exception where she had previously informed the tenant that she was tapping all incoming phone calls and, knowing this, the tenant used the phone anyway. The court held that implied consent could be found where the

surrounding circumstances showed "acquiescence or a comparable voluntary diminution of . . . otherwise protected rights." [119]

Title II of ECPA

Title II of the ECPA, the Stored Communications Act, makes it unlawful for one to access, obtain or alter or disclose contents of a stored electronic communication without proper authorization. [120] Like Title I, Title II contains an exception where consent has been given by one of the parties to the communication. [121] In addition, Title II specifically excepts conduct authorized by the entity providing the communications service or by the user. [122] An employer's accessing or monitoring activities will be excepted from its prohibitions where the employer is deemed to be the "entity providing a wire or electronic communications service," and authorizes its own monitoring activities. [123] In Bohach v. Reno, [124] for instance, the Court found that a city police department was a "service provider" and could not be liable under Title II because the department provided the terminals, computers, software and pagers which allowed users the ability to send or receive electronic communications. The city, "as the system provider, was free to access the stored messages as it pleased," the court said. [125]

Disclosure of stored communication is prohibited under Title II for entities providing "an electronic communication service to the public," [126] but there are exceptions similar to those in Title I for disclosures incident to provider services, [127] to protect the rights and property of the provider [128] or where the user consents. [129] In another case, a Title II claim for purported unlawful disclosure of e-mail to a newspaper was dismissed because the disclosing entity was not providing an "electronic communication service to the public," but only internally to another business. [130]

Disclosure to Authorities Under ECPA

Company disclosure to government agencies or authorities requires other precautions under 18 U.S.C. §2703. [131] If the data is stored fewer than 180 days, a provider of an electronic communication service may disclose e-mail or Internet content to the government only pursuant to a warrant, [132] and if stored more than 180 days, pursuant to a subpoena, court order or warrant depending on government notice to the subscriber or customer. [133] There are significant differences in the level of proof required, with the standard for the government to obtain a probable cause warrant being higher than that for a court order, [134] and a subpoena issuable by Asst. U.S. Attorneys or state attorneys often in their discretion. The Department of Justice apparently takes the position that §2703 applies only to service providers to the public and not to employers providing only e-mail or Internet services internally, thus limiting the circumstances where the federal government seeks a warrant. The FBI revealed they have been using specialized access software, called "Carnivore," to obtain e-mail from ISP's unwilling or unable to comply with a court order.

An entity or its employees supplying information in accord with a subpoena, court order or warrant under §2703 is immunized from liability. [135] To avail themselves of this immunity, entities providing electronic communication services should consider obtaining a subpoena, or order warrant before disclosing e-mail or Internet content to local, state or federal authorities. This sometimes involves negotiation with authorities who, on occasion, may not be familiar with this statute or its requirements. Some service providers are now adopting internal policies for e-mail or internet disclosure to the government so as to insure proper content disclosure precautions.

The Communications Decency Act

The Communications Decency Act (CDA), [136] was passed as part of the Telecommunications Act of 1996,

and subjects to fine, imprisonment, and civil liability anyone who, by means of a telecommunications device: (1) makes, creates, or initiates the transmission of any communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten or harass another person; or (2) knowingly permits any telecommunications facility under his control to be used for this activity with intent that it be used for such activity. [137] These portions of the law have been upheld. [138]

Though the CDA was primarily enacted to protect children from inappropriate communications and images, employers might reasonably wonder whether they can be held liable under the CDA for harassing or indecent web communications generated by their employees. Unless there is employer indifference or reckless disregard of employee web use, the answer is almost certainly no; and, in addition, the law provides protection for those involved in screening Internet use for offensive material.

In 1997, the U.S. Supreme Court struck down as unconstitutional two key provisions of the CDA dealing with indecent communication to minors. [139] The Court found that these provisions relating to minors were facially over-broad and vague, and violated the First Amendment.

The Child Online Protection Act

To remedy the constitutional defects in the CDA, Congress passed the Child Online Protection Act (COPA), [140] which was to become effective in November, 1998. [141] A federal court in Pennsylvania enjoined enforcement of this statute, finding that COPA, like the CDA, was unconstitutional in violating the First Amendment rights of adults, [142] which injunction the Third Circuit Court of Appeals upheld. The COPA litigation is ongoing, and the Justice Department is reportedly committed to vigorously defending and upholding COPA. In addition to COPA, Congress passed the Children's On-line Privacy Protection Act (COPPA), [143] administered by the FTC and aimed at regulating unfair and deceptive practices in connection with the collection and use of personal information from and about children on the Internet.

Surviving Portions of the CDA

Employer monitoring or blocking pornographic and other offensive use of the Internet by its employees is encouraged by surviving portions of the CDA. Monitoring activities are included in a section entitled "Protection for private blocking and screening of offensive material," [144] which states: "It is the policy of the United States . . . to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." [145] Other provisions of the CDA provide protection for employers engaged in screening Internet use for offensive material. [146]

There are also several noteworthy CDA defenses which do not appear to be superceded by COPA. One CDA defense is that no entity will be held liable under the CDA for the actions (including threatening or harassing Internet communications) of an employee or agent unless that employee or agent was acting within the scope of his or her employment, and the enterprise (a) had knowledge of the conduct, authorized it or ratified it, or (b) recklessly disregarded it. [147] This defense, geared specifically towards employers, makes it almost impossible for a company with enforced policies prohibiting such offensive Internet conduct to be held in violation of the CDA by virtue of its employees' Web messages or content.

Defendants who are Internet "service providers," which is defined more broadly in the CDA [148] than the ECPA, will be able to take advantage of the immunity provisions of §230(c)(1) to bar not only defamation claims, but also those for negligence, emotional distress and breach of contract. [149] The reach of this defense for employers who are service or system providers has only begun to be explored.

It is also not a violation of the CDA to provide access or connection to a system "not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication." [150] This defense, however, does not apply if the person who provides access or connection to the system also owns or controls it.[151] Assuming that an employer does not own or control the system to which they are providing access, it should not be held in violation of the CDA for communications its employees send via that system.

The protections afforded by the CDA to web monitoring activities are so broad that one might argue that they would also protect a monitoring employer under the ECPA. The CDA specifically provides, however, that it should not be construed to impair the application of the ECPA, nor will it prevent enforcement of the CDA's "core" prohibitions or the enforcement of "consistent" state laws. [152] How the ECPA and surviving portions of CDA are to be read consistently remains to be seen. The CDA does, however, manifest a favorable Congressional intent toward the good faith screening of Internet use to prevent access to offensive material.

Anti-Spam Statutes

For employers looking to protect themselves from or block unsolicited junk e-mails, commonly known as "spam," there is a patchwork of federal and state laws on which companies may rely. For example, the Computer Fraud and Abuse Act [153] prohibits any person from intentionally accessing a computer without authorization, knowingly transmitting information, and as a result causing damage to the computer. This law has been effective in dealing with fraudulent misrepresentations and false information transmitted by spammers. [154] The statute does not, however, address rights to monitor or filter the massive flow of non-fraudulent, unsolicited commercial e-mail.

Some fourteen states have enacted legislation to deal with spam, [155] but these have limited reach because they only regulate messages with some nexus to the state (e.g., the message either originated from or was delivered to a computer in that state). The Telephone and Consumer Protection Act of 1991, [156] otherwise know as the "Junk Fax Law," protects telephone and fax recipients from unsolicited advertisements, unless the recipient expressly consents, but its applicability to e-mail is tenuous. [157] While the law is primarily directed at protecting residences, the FCC issued extensive implementing regulations, [158] some of which are relevant to business solicitation.

Courts have also looked to common law actions such as trespass to stop unsolicited e-mail. For example, in Compuserve v. Cyber Promotions, [159] an Ohio district court determined that Cyber Promotions's unsolicited bulk advertising was sufficiently problematic to be enjoined. In that case, CompuServe relied on the property concept of trespass to chattels to protect its computer systems from being used to send spam. A business implementing monitoring software to block spam may, ironically, be faced with a question as to whether state electronic communication or wiretap laws that require mutual consent to interception or use might impede such employer oversight efforts, i.e. the "spammer" does not consent. One response is that exceptions stated in these laws, such as the "normal course of employment" or "protection of the provider's rights and property" exclusions, allow such "spam" blocking activity.

Proposed Federal Legislation

There are a host of proposed federal bills addressing the ECPA and e-mail and Internet privacy issues and rights. Many are expected to be revived in the coming year. The Clinton administration and others

proposed legislation to amend the increasingly obsolete ECPA, so as to apply to hardware and software surveillance, and require that applications for e-mail interception court orders be pre-approved by high level Justice Department officials; mandate suppression of illegally seized e-mail; and institute annual compilation and publication of government e-mail monitoring. [160]

Other federal bills, such as the proposed Notice of Electronic Monitoring Act, [161] have been introduced to require "clear and conspicuous notice" by employers to employees of reading or monitoring their e-mail, unless the employee is engaged in conduct which violates the employer's or others' rights or harms the employer. This pending legislation would require, prior to monitoring, annual employer notices "reasonably calculated to provide actual notice" and which describe:

1) The means by which such monitoring will be accomplished and the kinds of information that will be obtained through such monitoring, including whether communications or computer usage not related to the employer's business are likely to be monitored; 2) the frequency of such monitoring; and 3) how information obtained by such monitoring will be stored, used, or disclosed. [162]

To the extent that such a statute would both legitimize employer e-mail and web monitoring and define common employer policy notices to employees, it would eliminate some of the uncertainty in this field. Questions have, however, been raised as to whether this proposed federal law would be the exclusive employee remedy or whether state law actions could still be brought.

The Federal Trade Commission has argued for greater consumer privacy protections with resultant proposed legislation, [163] and there are serious suggestions for a federal "Privacy Commission", to include on-line and workplace privacy. [164] A federal bill to prohibit Internet gambling, other than that regulated by states on a closed loop, subscriber based system, had moved to the House floor, [165] as did unsolicited e-mail bills. [166]

International Issues – U.S. Safe Harbor Agreement with E.U.

Among the most closely watched European developments is the new "Safe Harbor" Agreement [167] that limits the restrictions of the European Union Privacy Directive for U.S. firms seeking data from Europe. Employers with operations in Europe or those obtaining customer, marketing or personnel information from Europe should pay close attention to these issues. U.S. companies receiving personal data from E.U. firms will now need to decide on compliance, which may be burdensome, including whether they are willing to adopt and institute so-called "privacy" policies, consistent with U.S. law. As of Nov. 1, 2000 U.S. companies may decide whether they wish to participate voluntarily in the Safe Harbor Agreement and, if so, inform the Department of Commerce as to means of compliance, [168] with the Federal Trade Commission overseeing enforcement. The Dept. of Commerce has established a web site ‹http:www.export.gov/safeharbor› to explain the agreement and to allow U.S. companies to enroll online.

The fifteen member states of the European Union adopted Privacy Directive 95/46, effective October, 1998 which guarantees privacy for individuals with respect to the processing of personal data. The Directive defines "personal data" as "any information relating to an identified or identifiable natural person... who can be identified, directly or indirectly by reference to an identification number." [169] Under the Directive, such data may not be collected, recorded, or blocked unless the data subject has "unambiguously consented." [170] The data subject can consent to data processing only after being informed of the identity of the data controller, the purposes of the data processing, and the recipients of the data. [171] Directive 95/46 does not mention or refer to European employer oversight of its employees' e-mail or

Internet usage but it has been interpreted to encompass electronic data transfers. Some countries like Canada, Australia and Argentina have already enacted new privacy legislation to comply with the E.U. Directive.

The European Union and U.S. Dept. of Commerce in March, 2000 reached agreement on "safe harbor" principles for U.S. companies to resolve disputes over individual privacy in European data transmissions to U.S. firms. The agreement was published in final form by the Dept. of Commerce on July 21, 2000. [172] The EU Privacy Directive limits or curtails EU companies in transferring personal data, such as personnel, marketing or medical information, to companies in the United States and elsewhere unless U.S. companies provide "adequate" privacy protection. The United States proposed that the EU offer "safe harbor" from coverage or obligations under the EU directive to U.S. companies who agree with certain privacy principles, [173] and the E.U. did not interrupt data flows to the U.S. during the protracted negotiations. Dept. of Commerce officials negotiated so that U.S. companies could comply with the otherwise strict EU directive by:

- adopting a "privacy" policy, consistent with EU Privacy Directive Principles, including an internal means for handling privacy complaints and showing that they were adequately already covered by U.S. privacy laws;
- identifying regulatory bodies that have authority over such disputes with the company;
- obtaining membership in bodies like TRUSTe or BBBOnline, which is a Better Business Bureau program monitored by the FTC.

If human resource information is to be transferred from E.U. countries, the participating U.S. company must agree to mechanisms to resolve individual privacy disputes, including cooperation with European data protection commissioners or "DPA's." [174] These obligations and the exceptions are explained in the agreement in part by so-called Frequently Asked Questions or FAQ's.

Failure to enter or adhere to this program may subject U.S. companies to arduous enforcement actions by E.U. member state authorities. Tensions between European and American views on employee privacy are very real. The European Parliament unexpectedly voted to reject the "Safe Harbor" Agreement in early July, 2000, reportedly insisting on more stringent privacy restrictions for U.S. companies. [175] The European Commission overruled this action and notified the United States that it will proceed with the "Safe Harbor" Agreement as planned. [176] A group of major U.S. corporations banded together to oppose the "Safe Harbor" agreement as too costly and a bureaucratic imposition. [177]

Adjusting to these European privacy norms, even by way of the safe harbors, will create significant administrative burdens for U.S. companies, including possible segregation of European data and/or necessity to appoint a privacy officer. Such policies will require further modification or special versions of U.S. companies' e-mail and internet policies.

Conclusion

The "law" pertaining to e-mail and Internet issues in the workplace is rapidly evolving, and employers — and their counsel — should do their best to stay abreast of the current law and legislation in this area. Companies without an e-mail and Internet use and monitoring policy should implement one, tailored to their needs and consistent with their workplace and discipline mode. While such policies may not insulate employers from liability, companies with policies are likely to fare better in litigation and such policies will at least provide guidance on employee conduct and the extent of reasonable and expected monitoring when employee dilemmas arise—as they inevitably will. ■

APPENDIX

1 Elron Software Corp., 1999 Workplace E-mail Abuse Study (March 1,1999) ‹http://www.elronsw.com/press/survey.htm›; Elron Software Corp., 1998 Workplace Internet Surf Abuse Study (June 1,1998) ‹http://www.elronsw.com/press/survey.htm›.

2 Susan Gindin, Guide to E-Mail and the Internet in the Workplace, Corporate Counsel Daily News: Corporate Practice Series (BNA) (March 9,1999) ("Gindin").

3 See Robert Hersey, Jr., Some Abandon the Water Cooler for Stock Trading on the Internet, N.Y. Times, May 20, 1999, at 1.

4 "Spam" has various definitions but is usually considered to be unsolicited commercial e-mail, used as part of a marketing or sales campaign of the spammer, and not sent at the request of or with the consent of the recipient. See Scott M. Jensen, Unsolicited Electronic Mail: New Laws Would Reduce Our Spam Intake, Cyberspace Lawyer, May 1998, at 2-3.

5 Jefferey Rosen, The Eroded Self, N.Y. Times Mag., May 2, 2000.

6 Notice of Electronic Monitoring Act, H.R. 4908 (2000) and S. 2898 (2000).

7 Id. at proposed §2711(a).

8 See Dan Small, Wired Justice: Lure and Danger of E-Mail, MSNBC Opinions, (posted February 9, 1999), ‹www.msnbc.com/news/238803.asp›.

9 See Ross Kerber, On-Line Fallout from Raytheon Search Reportedly Claims Second Worker, Boston Globe, April 2, 1999, at E1, available in 1999 WL 6055513, and follow-up stories, Boston Globe, April 5, 1999, at A1, and April 9, 1999, at C1, available in 1999 WL 6055686 and 6056624.

10 Boston Globe, Sept. 21, 2000, at C11.

11 Suspect in Emulex Case Worked for Internet Wire - FBI, Reuters (Aug. 21, 2000), ‹http://dailynews.yahoo.com/h/nm/20000831/ts/emulex_arrest_dc.html›.

13 Two Plead Guilty, SEC Expands Charges in Online Stock Price Manipulation Case, Internet. Regulation. Alert 11 (Pike & Fischer) (July 14, 2000).

14 Id.

15 See Owens v. Morgan Stanley & Co. Inc., No.96 Civ. 9747, 1997 WL 403454 (S.D.N.Y. 1997); see Michelle Singletary, Loose Lips an E-Mail Hazard, Newsday, April 6, 1997, at F12.

16 928 F. Supp. 533 (E.D. Pa. 1996).

17 See also Williamson v. DiMaio, 1999 U.S. Dist. Lexis 5430 (E.D.N.Y. April 15, 1999).

18 80 F. Supp.2d 1342, 1344 (S.D. Fla. 2000); see also Wilson-Simmons v. Lake County Sheriff's Dept., 982 F. Supp. 496 (N.D. Ohio 1997).

19 No. CIVA95CV716(RSP/GJD), 1990 WL 166845 (N.D.N.Y. 1998).

20 No. Civ. A. 96-5987, 1997 WL 634501 (E.D. Pa. 1997).

21 93 F.3d 1327 (7th Cir. 1996).

22 Id. at 1330.

23 See Daniels v. WorldCom Corp., No. Civ. A 3197-CV-0721-P, 1998 WL 91261 (N.D. Tex. Feb. 23, 1998).

24 51 F.3d 372 (2nd Cir. 1995), on remand at NO. 92 CIV. 7126 KTD, 1999 WL 604871 (S.D. N.Y. Aug. 10, 1999) (granting defendant's motion for judgment as a matter of law).

25 992 F. Supp. 644 (S.D. N.Y. 1998).

26 164 N.J. 38, 751 A.2d 538 (2000).

27 Communications Decency Act, 47 U.S.C. §223(e)(4). See pp.89- 91, infra, for discussion of CDA.

28 Id. at §230(c)(1) ("No provider or user of any interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); see Blumenthal v. Drudge, 992 F. Supp. 44, 49-53 (D. D.C. 1998)(immunity for ISP's for defamation under this section).

29 No. COA 99-162, 2000 WL 108504 (N.C. App. Feb. 1, 2000).

30 983 F. Supp. 1167 (N.D. Ill. 1997).

31 See Digital Millennium Copyright Act, Pub. L. 105-304; No Electronic Theft Act, Pub. L. 105-`47; Economic Espionage Act, Pub. L. 104-294; and amendments to 18 U.S.C. §1030. See also Moulton v. VC3, 6 I.L.R. (P&F) 3096 (N.D. Ga. 2000) and John K. Markey and James F. Boyle, New Crimes of the Information Age, 43 Boston Bar. J. 10 (May/June, 1999).

32 331 N.L.R.B. No. 40 (2000).

33 Pratt & Witney, 26 AMR 36322, 1998 NLRB GCM Lexis 40 (Feb. 23, 1998); see IRIS-USA, 32-CA-17763, 2000 WL 2571078 (Feb. 2, 2000).

34 311 N.L.R.B. No. 893 (1993).

35 323 N.L.R.B. No. 30 (1997).

36 For an interesting discussion of these and other union issues, see Kenneth R. Dolin and Scott Rozmus, Regulating Employee E-Mail, National Law Journal, July 31, 2000 at B5.

37 See James Bardler, Harvard Ouster Linked to Porn, Boston Globe, May 19, 1999 at B1.

38 Id. at B5.

39 For a discussion on the consent defense, see text accompanying footnotes 114 to 119.

40 For other policy templates, see Elron Software, Internet Policy Administration Guide, at 21 ("Elron Internet Guide"), ‹www.elronsoftware.com›; Michael R. Overly, E-POLICY, at 99-106 (AMA-COM, 2000); 21 InfoWorld, Issue 36, Enterprise Careers, Guidelines for Setting Sound Policy, Monday Sept. 6, 1999, 1999 WL 21901260; Commonwealth of Massachusetts Administration and Finance Policy on the Use of Information Technology Resources (June 16, 1998).

41 See Edward Jones Fires 19 for Failing to Admit E-Mail Improprieties, N.Y. Times, May 10, 1999.

42 See, Nick Wingfield, More Companies Monitor Employees' E-Mail, Wall St. J., Dec. 2, 1999, at B8.

43 Id.

44 Elron Software, Internet Policy Guide Administration Guide, ‹http://www.elronsoftware.com›.

45 See G.L.M. c.149 §52C, under which "personnel records" of Massachusetts employers are subject to three year or longer retention periods; and 29 CFR §1602.14, EEOC regulation requiring personnel records, applications, hiring, promotion, transfer and termination information, to be kept for one year.

46 Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106 – 229. The statute is, for the most part, effective October 1, 2000, but is effective on March 1, 2001 with respect to record retention requirements imposed by state or Federal agencies or regulations.

47 In addition, regulated services, such as financial, banking, healthcare and law practice, must implement mechanisms to avoid breaches of confidentiality. See, e.g., ABA Comm. on Ethics and Professional Responsibility, Formal Op. 99-413 (1999) (lawyers may transmit client information by unencrypted e-mail without violating the Model Rules of Professional Conduct because the mode of transmission affords a reasonable expectation of privacy); Massachusetts Bar Association Ethics Op. 94-5 (possible waiver of attorney-client and work product privileges); see also Ohio Bd. Com. Griev. Disp., Op. 99-2, 1999 WL 231598 (1999) (lawyers do not violate the duty to preserve confidence by communicating with clients through unencrypted electronic mail).

48 In general, computer data including backup tapes that may contain old e-mail messages and messages that were supposedly deleted, are discoverable in state and federal court litigation. In fact, "today it is black letter law that computerized data is recoverable if relevant." Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934, at *2 (S.D.N.Y. 1995). FRCP 34 and the corresponding Advisory Committee Notes mandate that electronic data compilations be discoverable in litigation. Rule 34 be obtained only with the use of detection devices. See Crown Life Insurance Co. v. Craig, 995 F.2d 1376 (7th Cir. 1993) ("Rule 34 contemplates that when data is in an inaccessible form, the party responding to the request for documents must make the data available.").

49 Linnen v. A.H. Robbins Co., No. 97-2307, 1999 WL 462015 at * 11 (Mass. Super. Ct. Jun. 16, 1999).

50 179 F.R.D. 622 (D. Utah 1998).

51 In Gates Rubber Co. v. Bando Chemical Industries, Ltd. 167 F.R.D. 90 (D. Colo. 1996), the plaintiff's computer expert used Norton's "Unerase" software program to attempt to retrieve previously "deleted" files from the defendant's computer system. The plaintiff was able to recover "deleted" files in this way. However, courts have been more reluctant to allow plaintiffs unfettered access to employer's computer files. In Fennell v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996), the plaintiff alleged that she had been unlawfully discharged by her employer in retaliation for making a sexual harassment complaint. The plaintiff sought additional discovery of the defendant's computer files in the hope that she might find evidence that a particular document, which was central to the dispute, was fabricated by the defendant. The First Circuit affirmed the District Court's denial of the request for additional discovery, stating that the plaintiff had not demonstrated "a particularized likelihood of discovering appropriate information."

52 Linnen, 1999 WL 462015 at *6. See also Bills v. Kennecott Corp., 108 F.R.D. 459 (D. Utah 1985) (parties should not be denied access to discoverable computer data merely because of format in which it is stored).

53 No. 94 C 897, MDL 997, 1995 WL 360526 at *2 (N.D. Ill. Jun. 15, 1995).

54 No. 96 C 7276, 1997 U.S. Dist. LEXIS 7980 (N.D. Ill. Jun. 5, 1997).

55 See Mathew Brelis, Getting Caught, Boston Globe, May 30, 1999, at E-2.

56 Section 1B of G.L.M. c.214 provides that "a person shall have a right against unreasonable, substantial, or serious interference with his privacy."

57 R.I. Gen. Laws § 9-1-28.1 (1999); see also Pontbriand v. Sundlun, 699 A.2d 856, 863 (R.I. 1997) (statutory right to privacy; no common law right to privacy in Rhode Island); New York Civ. Rights Law § 50 (McKinney 1992); see also Messenger v. Gruner and Jahr Printing and Publishing, No. 01705, 2000 WL 190553 (N.Y. 2000) (statutory right of privacy; New York does not recognize a common law right of privacy); Va. Code Ann. § 801-40(A); see also Williams v. Newsweek, Inc., 63 F. Supp.2d 734, 736 (E.D. Va. 1999) ("[t]his statute provides the only remedy under Virginia law for a claim of invasion of privacy).

58 The other three types of invasion of privacy claims are: (1) appropriation of another's name or likeness; (2) unreasonable publicity given to another's private life; and (3) publicity that places another in false light before the public. Restatement (Second) of Torts §652A (1977).

59 Restatement (Second) of Torts §652B (1977).

60 See Stewart v. The Pantry Inc., 4 IER Cases 526, 532 (W.D. Ky. 1988) ("consent…is a complete defense"); WalMart, Inc. v. Stewart, 15 IER Cases 1270, 1274 and 1275 (Alaska 1999) (discussing the employer's consent defense, trial court instructed the jury "that any search to which [the employee] had voluntarily consented could not be considered an offensive intrusion"); Hill v. NCAA, 865 P.2d 633, 657 (Cal. 1994) (a defendant to a California constitutional privacy claim "may … plead and prove other available defenses, e.g., consent … that may be appropriate in view of the nature of the claim and the relief requested"). But see, Kraslawsky v. Upper Deck Co., 12 IER Cases 1789, 1796 (Cal. Ct. App. 1997) ("consent is generally viewed as a factor in the balancing analysis and not as a complete defense to a privacy claim").

61 Stewart v. The Pantry, Inc., 4 IER Cases 526, 528 and 532.

62 C.A. No. 95-2125 (Middlesex (Mass.) Super. Ct., Memorandum dated August 12, 1996), 5 Mass. L. Rptr. No. 31,712 (Nov. 4, 1996).

63 G.L.M. c.214, §1B. For a discussion of the Massachusetts wire-tap statute in this case and the recent decision of Dillon v. Massachusetts Bay Transit Authority, 49 Mass. App. Ct. 309 (2000), see text accompanying footnote 89-91.

64 5 Mass. L. Rptr. No. 31,712 at 31,714.

65 Employer Successfully Defends E-Mail Privacy-Invasion Case, 28 Massachusetts Lawyers Weekly 983 (January 10, 2000).

66 Employment Wrongful Termination – Invasion of Privacy – Employer Reading Employee E-Mail, 28 Massachusetts Lawyers Weekly 873 (December 20, 1999).

67 No. BO68705 [1 ILR (P&F) 109] (Cal. Ct. App. July 26, 1996), ‹www.loundy.com/CASES/Bourke_v_Nissan.html›.

68 206 F.3d. 392 (4th Cir. 2000).

69 29 F. Supp.2d 324 (E.D. Va. 1998).

70 914 F. Supp. 97 (E.D. Pa. 1996).

71 Id. at 101.

72 No. 05-97-00824-CV, 1999 WL 339015, at *1 (Tex. Civ. App. May 28, 1999).

73 Id. at *4.

74 Ala. Code 13A-11-8; Conn. Gen. Stat. 53A-182B; Del. Code Ann. tit. 11 1311; Ind. Code 35-45-2-2; N.Y. Penal Law 240.30; Wisc. Stat. §947.0127.

75 Fla. Stat. Ann. §934.103(2)(d) (West 1999); Md. Code Ann., §10-402(c)(3) (1999).

76 Fla. Stat. Ann. §934.03(4); Md. Code. Ann. §10-402(b).

77 Colo. Rev. Stat. Ann. §24-72-204.5(1) (West 1999).

78 Wis. Stat. Ann. §230.86(1) (West 1999).

79 1999 H.B. 2657. The bill proposed to require employers to inform employees of the types and frequency of electronic monitoring that the employer uses, and what data identifiable to a particular employee will be collected; to provide a full description of how information will be used; and to inform prospective employees of monitoring that may affect the prospective employee if hired. See Frank Phillips, House OK's Bill Aimed At E-Mail Stalkers, Boston Globe, July 13, 2000 at B2.

80 See Comm. of Mass. Exec. Order No. 412, "To Protect the Privacy of Personal Information" (June 23, 1999).

81 SPR Bulletin, No. 1-99 (Feb. 16, 1999), published by William Francis Galvin, Secretary of the Commonwealth, Massachusetts State Archives;

‹http://www.magnet.state.ma.us/sec/arc/arcmu/spr9901.htm.›

82 G.L.M. c.66. In November 1996 the Middlesex District Attorney's Office issued Guidelines for Use of E-Mail by Members of Governmental Bodies, stating that e-mail communications among a quorum of a governmental board or committee that relate to public business would violate the Open Meeting Law, G.L.M. c. 39, §§23A-24.

83 Id. at c.4, §7(26)(A-M).

84 Commonwealth of Massachusetts Administration and Finance Policy on the Use of Information Technology Resources, ¶9 (June 16, 1998).

85 C.A. No. 95-2125 (Middlesex (Mass.) Super. Ct., Memorandum dated August 12, 1996), 5 Mass. L. Rptr. No. 31,712 (Nov. 4, 1996).

86 G.L.M. c. 272, § 99.

87 A recent Massachusetts court dealt with a similar argument, albeit in the criminal context, in Commonwealth v. Accetta, Crim. No. 99-275, 28 Mass. Lawyers Weekly 611 (Middlesex (Mass.) Super. Ct.; Fremont Smith, J. 1999). The defendant, accused of sending illegal sexual e-mail messages to a minor, made a motion to suppress the messages, arguing that the state anti-wiretapping statute prevented the minor's father from intercepting the e-mails and prevented the Commonwealth from introducing the messages into evidence. In denying the defendant's motion, the court stated that suppressing the evidence would contravene public policy. The court did not, however, reach the issue of whether the father's "interception" was an act that was excepted from the anti-wiretapping statute.

88 G.L.M. c.272, §99(D)(1)(b).

89 49 Mass. App. Ct. 309 (2000).

90 Id., at 314-16.

91 Id., at 311.

92 No. BC007036, slip op. (Cal. Super. Ct. Jan. 4, 1991).

93 The California wiretap statute prohibits a person from "intentionally tap[ping] , or mak[ing] any unauthorized connection … with any telegraph or telephone wire, line, cable, or instrument, or read[ing], or attempt[ing] to read, or to learn the contents of any message, report, or communication while the same is in transit or passing over any wire, line or cable…." Cal. Penal Code §631. The statute makes such conduct illegal and also provides for a civil cause of action for persons aggrieved by such conduct. See id. at §§631 and 637.2.

94 See No. BC007036, slip op. at 2. 95 No. BO68705 [1 ILR (P&F) 109] (Cal. Ct. App. July 26, 1996), ‹www.loundy.com/CASES/Bourke_v_Nissan.html›.

96 See Cal. Penal Code §631.

97 No. BO68705 [1 ILR (P&F) 109] (Cal. Ct. App. July 26, 1996), ‹www.loundy.com/CASES/Bourke_v_Nissan.html›.

98 18 U.S.C. §2510 et seq.

99 Steve Jackson Games v. U.S. Secret Service, 36 F.3d 457, 462 (5th Cir. 1994); cited also in United States v. Moriarty, 962 F. Supp. 217, 221 (D. Mass. 1997) (discussing ECPA).

100 See text accompanying footnotes 160 to 162.

101 18 U.S.C. §2511(2)(d); see Jennifer L. Dean and Ned T. Mimmedrich, Stay Out of the Inbox (May 21, 1999) ‹http.//www.lawnewsnetwork.com/practice/techlaw/papers/lawfirm/A1663-1999May 21.html›.

102 18 U.S.C. §2510(5)(a)(ii).

103 U.S.C. §2511(2)(a)(i). A discussion of these defenses is beyond the scope of this article and may be found elsewhere. See generally Judith Lockhart, Gerald W. Griffin, Monitoring Employee E-mail, Voice Mail and Computer Files Without Violating Employees' Privacy Rights, November 8, 1999, ‹http://www.clm.com/pubs/pub-9144477_ 1.html›; Garry G. Mathiason, Michelle R. Barrett, The Electronic Workplace: Employment Law Implications and Solutions; Privacy in the Electronic Workplace, ‹http://prof.findlaw.com/electronic/electronic_11.html›; Thomas R. Greenberg, E-Mail and Voicemail: Employee Privacy and The Federal Wiretap Statute, 44 Amer. U.L. Rev. 219 (1994); Larry O. Natt Gantt, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 Harv. J.L. & Tech. 345, 359 (1995) (suggesting that exception would apply to employer providers); Gindin at 25-29 (same); but see Julia T. Baumhart, The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?, 8 Lab. Law 923, 936 (1992) (suggesting limiting exception to public Internet service providers such as AOL).

104 Victoria C. Shapiro, Privacy and the Internet, ‹http://Internet-law.pf.com›/Subjects Covered/Privacy/Overview›.

105 Giddens v. S&A Restaurant Corp., No. 97C 3101 (N.D. Ill. 2000); discussed in James A. Burstein and William F. Dugan, Employers on the Offensive: Combating Improper Employee Use of Voice Mail and Electronic Mail Systems. 26 Employee Relations L.J. 89 (Autumn, 2000). See also Lopez v. First Union Nat. Bank of Florida, 129 F.3d 1186, 1189-1190 (11th Cir. 1997).

106 18 U.S.C. §2511(1)(a).

107 Id. at §2511(1)(c).

108 Id. at §2511(1)(d). To avoid improperly "intercepting" an "electronic communication," it is important to understand how these terms are defined by the Act. An "electronic communication" is broadly defined to include the transfer of any writing, images, sounds or intelligence of any nature, by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. Id. at §2510(12). "Intercept[ion]" is defined as the aural or other "acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device." Id. at §2510(4).

109 Id. at §2511(4)(a) and §2520. Civilly, violators of the ECPA can be held liable for the greater of actual damages or statutory damages of $100 a day for each day of violation or $10,000. Id. at §2520(c)(2). Violators also face the possibility of punitive damages, reasonable attorney's fees and litigation costs. Id. at §2520(b).

110 See U.S. v. Smith, 155 F.3d 1051, 1055-59 (9th Cir. 1988); U.S. v. Moriarty, 962 F. Supp. 217, 220 (D. Mass. 1997), Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997); Bohach v. Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996); U.S. v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996); Jackson Games, Inc. v. U.S. Secret Service, supra.

111 Moriarty, 962 F. Supp. at 220-221; Bohach, supra, 932 F. Supp. at 1236.

112 18 U.S.C. §2510(4).

113 See text accompanying footnotes 136-139, 144-152, for discussion of CDA.

114 18 U.S.C. §2511(2)(d).

115 C.A. No. 00-472, 2000 U.S. Dist. Lexis 4276 (E.D.Pa. 2000).

116 Though it cites no support for the proposition, the First Circuit stated that under the old federal wiretap statute "there is no implied consent exemption." Campiti v. Walonis, 611 F.2d 387, 396 (1st Cir. 1979). This statement is contradicted by subsequent cases such as Griffin v. Milwaukee, 74F.3d 824, 827 (7th Cir. 1996) and Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990).

117 U.S. v. Kennedy, 81 F.Supp. 2d 1103, 1110 (D.Kan. 2000).

118 904 F.2d 112 (1st Cir. 1990).

119 Id. at 116. In cases where a party knows only that business, but not necessarily personal, calls might be monitored, the existence of implied consent is less clear. The employer in Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983), was unable to rely on the consent exception to excuse its acknowledged interception of an employee's personal phone call where the employer's established monitoring policy was limited to the monitoring of business calls only.

120 18 U.S.C. §§2701(a) and 2702(a). It too provides a civil remedy which may include actual damages, but not less than $1,000, for willful or intentional violations, and litigation costs including attorneys' fees. Id. at §2707.

121 Id. at §2702(b)(3).

122 Id. at §2701(c).

123 Id. at §2701(c)(1).

124 932 F. Supp. 1232, 1236 (D. Nev. 1996).

125 Id. at 1236.

126 18 U.S.C. at §2702(a)(1).

127 Id. at §2702(b)(5).

128 Id.

129 Id. at §2702(b)(3).

130 Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. I11). 1998).

131 See U.S. v. Kennedy, 81 F.Supp. 2d 1103 (D.Kan. 2000) (court order defective but suppression not remedy); In Re: United States, 36 F.Supp. 2d 430 (D.Mass. 1999) (discussing disclosure requirements); McVeigh v. Cohen, 983 F.Supp. 215 (D.D.C. 1998) (Navy violated ECPA in orally obtaining information from AOL).

132 Id. at §2703(a).

133 Id. at §2703(a) and (b). Entities providing "remote computing services" have similar obligations depending on whether notice was given to the customer or subscriber. Id. at §2703(b).

134 A court order under §2703 is to be issued under an "intermediate standard," higher than a subpoena but lower than a probable cause warrant. Kennedy, 81 F.Supp. 2d at 1109 n.8.

135 18 U.S.C. §2703(e). There is also an exclusion for disclosures to

law enforcement if the content was "inadvertently obtained by the service provider" and appear to pertain to a crime. Id. at §2702(b)(6).

136 47 U.S.C. §223.

137 Id. at §223(a).

138 See Apollomedia Corp. v. Reno, 19 F. Supp. 2d 1081 (N.D. Cal. 1998), aff'd, 526 U.S. 1061 (1999).

139 ACLU v. Reno, 521 U.S. 844 (1997). The first provision struck down (47 U.S.C. §223(a)(1)(B)) had prohibited the transmission of a communication which is indecent, with knowledge that the recipient is under 18 years old. The other provision deemed unconstitutional (47 U.S.C. §223(d)(1)) had prohibited a person from sending or displaying via an interactive computer service to one under 18 years old any communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs. The Court reached its conclusion by considering both the language and structure of the CDA, as well as the nature and function of the Internet, finding that the CDA's "indecent transmission" and "patently offensive display" language was vague and abridged the freedom of speech. See id. at 871. The Court reasoned that the federal government's interest in protecting children from harmful materials did not justify an unnecessarily broad suppression of speech addressed to adults, where there were other possible, less restrictive ways to protect minors. See id.

at 875, 879. The Court also found that the CDA's defenses did not cure the Act's defects. The defense requiring good faith, reasonable, effective, and appropriate actions to prevent access by minors (47 U.S.C. §223(e)(5)(A)) was deemed illusory given that current technology does not permit effective access prevention. Reno, 521 U.S. at 881. The defense requiring use of a verified credit card or adult identification number (47 U.S.C. §223(e)(5)(B)) was also discarded, because commercial providers of sexually explicit material already employ such tactics, there is no proof that they actually work, and it is not economically feasible for non-commercial speakers to employ such techniques. Reno, 521 U.S. at 882.

140 47 U.S.C. §231.

141 COPA subjects to fine, imprisonment and civil liability anyone who knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor under 17 years old and that includes material harmful to a minor. 47 U.S.C. §231(a). Entities excluded from liability under COPA include (1) telecommunications carriers engaged in the provision of telecommunications services; (2) a person engaged in the business of providing an Internet access service or (3) Internet information location tool; or (4) one similarly engaged in the transmission, storage, retrieval, hosting, formatting or translation of a communication made by another person, without selection or alteration of the content of the communication. 47 U.S.C.§231(b). COPA provides affirmative defenses, including that the defendant, in good faith, has restricted access by minors to harmful material by (A) requiring the use of a credit card, debit account, adult access code, or adult personal identification number; (B) accepting a dig ital certificate that verifies age; or (C) any other reasonable measures that are feasible under available technology. 47 U.S.C. §231(c)(1).

142 ACLU v. Reno, 31 F. Supp.2d 473 (E.D. Pa. 1999), aff'd., 217 F.3d 162 (2000). See also U.S. v. Mento, 2000 U.S. App. LEXIS 27869, 2000 WL 1648878 (4th Cir. (Md.)) (upholding constitutionality of Child Pornography Proctection Act of 1996).

143 15 U.S.C. §6502; see implementing regulations, 16 C.F.R. §312, effective April 21, 2000, 64 Fed. Reg. 59887 (1999).

144 47 U.S.C. §230.

145 Id. at §230(b)(4).

146 One provision specifically states that no claim may be brought on account of activity that is not a violation of law, "which that entity has taken in good faith to implement a defense authorized under this section or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section." Id. at §223(f)(1). In addition, the act's protection of "good samaritans" who attempt to block and screen offensive material is not limited to the protection of minors. This "good samaritans" protection is in two parts. The first provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. at §230(c)(1). Several definitions are required to understand this sentence. An "interactive computer service" is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet." Id. at §230(f)(2). An "information content provider" is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." Id. at §230(f)(3). Finally, "access software" is defined to include tools that enable a user to filter, screen, allow or disallow content, receive, display, search or organize content. Id. at §223(h)(2). Thus an employer will not be treated as the publisher of information sent by its employees where those employees are not acting within the scope of their authority. Second, the act broadly limits the civil liability of providers and users of interactive computer services for: (a) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; and (b) enabling information content providers to similarly restrict access or material. Id. at. §230(c)(2).

147 Id. at §223(e)(4).

148 Id. at §230(f)(2) ("Any information service, system, or access software provider that provides or enables access by multiple users to a computer service.")

149 See Jane Doe v. Lisa Oliver, 2000 Conn. Super. Lexis 570; Blumenthal v. Drudge, 992 F. Supp. at 49-53.

150 Id. at §223(e)(1).

151 Id.

152 Id. at §230(e)(1), (3), (4).

153 18 U.S.C. §1030.

154 See Hotmail Corporation v. Van$ & Money Pie, Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *2 (N.D. Cal April 16, 1998).

155 ‹http://www.jmls.edu/cyber/statutes/email/state.html›; See also Max P. Ochoa, Legislative Note: Recent State Laws Regulating Unsolicited Electronic Mail, 16 Santa Clara Computer & High Tech. L. J. 459, 471 n.12 (May, 2000) (collecting state statutes). A California court recently ruled that California's anti-spam law violated the Commerce Clause of the U.S. Constitution. Ferguson v. Friedlander, Inc., 5 ILR (P&F) 3067 (Cal. Super. Ct. 2000). Massachusetts proposed legislation in 1997 and 1999 which would have prohibited intrastate commercial e-mail messages, but the bills died in committee. HB 4581 (Mass. 1997) and HB 4104 (Mass. 1999).

156 47 U.S.C. §227.

157 See Unsolicited Electronic Mail; New laws Would Reduce Our Spam Intake, 3 Cyberspace Lawyer 2 (May, 1998); David E. Sorkin, Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991, 45 Buffalo L. Rev. 1001 (1997).

158 47 C.F.R. 64 1200.

159 962 F.Supp. 1015 (S.D. Ohio 1997).

160 The Electronic Communications Privacy Act of 2000, H.R. 5018, and the Digital Privacy Act of 2000, H.R. 4987; see Clinton Administration to Advance Bill to Update Wiretapping, Eavesdropping Laws, 2 Internet. Regulation.Alert 1 (Pike & Fischer) (July 21, 2000).

161 H.R. 4908 (2000) and §. 2898 (2000).

162 H.R. 4908, proposed §2711(b)(2)-(4). Civil actions could be brought for actual damages, but not less than liquidated damages of $5,000, nor more than $20,000 per employee or more than an aggregate amount of $500,000 against one employer. Id. at proposed §2711(d).

163 S. 2606 (2000) and H.R. 4611 (2000).

164 H.R. 4049 (2000).

165 H.R. 3125-RH; see Goodlatte, Tauzin Reach Compromise On Measure To Prohibit Internet Gambling, 2 Internet.Regulation.Alert 4 (Pike & Fischer) (July 14, 2000).

166 H.R. 4271 and 3113 (2000); S. 2928 and 2542 (2000).

167 65 Fed. Reg. 56534 (Sept.19, 2000); 65 Fed. Reg. 45666 (July 24, 2000).

168 Id.; see E.U. - US Safe Harbor Protection Agreement, (Sept. 29, 2000), ‹http://www.gdlaw.com/publications/uploads/safeharbor.asp›. Whether U.S. financial services companies can participate is still being negotiated. See 2 Internet.Regulation.Alert 6 (Pike & Fischer) (Dec. 8, 2000).

169 See, Directive 95/46/EC, ch. I, art. 2(a), 1995 O.J. L281 (Oct. 24, 1995), ‹http://www.doc.gov/ecommerce/eudir.htm›.

170 Id. at ch. I, art. 2(b).

171 Id. at ch. II, art. 10.

172 65 Fed Reg. 45666. (July 24, 2000).

173 65 Fed. Reg. 45666, 45669-70.

174 65 Fed Reg 45666, 45669-70 (FAQ 6).

175 EU Parliament, U.S. Congress Seek to Move Goal Posts on U.S. Privacy, Alston & Bird LLP Electronic Commerce Advisory (July 6, 2000) ‹http://www.alston.com/docs/advisories/199709/euparliament. htm›.

176 EU Assures U.S. It Will Honor Privacy Pact Despite Rejection By European Parliament, 2 Internet.Regulation.Alert 3 (Pike & Fischer) (July 28, 2000).

177 Brandon Mitchner, EU Privacy Rules Carry A Cost, Wall Street Journal Interactive Edition (April 4, 2000), ‹http://interactive.wsj.com/archive/retrieve›.

ELRON
SOFTWARE

Elron Software, Inc. · 7 New England Executive Park · Burlington, MA 01803 · Tel: (781) 993-6000 · Fax: (781) 993-6001

LEGALWP7/01DM 011-BKL-0057