NOTE

Electronic Communications and the Law: Help or Hindrance to Telecommuting?

Jennifer C. Dombrow[*]

I. Introduction

Telecommuting is generally defined as "moving the work to the workers instead of moving the workers to work."[1] Telecommuting represents how an estimated 11.1 million workers performed some of their work in 1997.[2] These workers responded to electronic mail (e-mail) messages from supervisors and clients regarding current projects, read e-mail messages from co-workers, and answered telephone calls forwarded from the office. They worked on client accounts while connected to their company's computer network system and wrote memos to other company personnel, which were sent via an electronic communications system. Other workers reported to a remote work center closer to their homes than the actual company premises. This allowed them to commute, on average, half the distance while producing the same or an increased volume of work. The use of telecommuting may range from simply performing work at home to connecting with other employees via electronic communications. A computer connection dramatically increases the amount of work that can be done away from the office.

The capacity to telecommute positively correlates with advances in supporting technology.[3] While the benefits of telecommuting are apparent to both employees and employers, the use of electronic communications in the workplace concerns employers regarding potential problems such as fraud, copyright infringement, loss of trade secrets, sabotage, violations of business policy, and other illegal conduct.[4] Last year for example, two employees of Morgan Stanley filed a racial discrimination suit against the firm for a series of racially offensive jokes circulated over the corporate

network.[5]

Protection against such activities occurring in the workplace is especially important as electronic communications are now being used as evidence in litigation. For instance, in *Strauss v. Microsoft Corp.*,[6] the court relied in part on e-mail messages containing sexual innuendoes to deny Microsoft's motion for summary judgment. The messages helped to create a genuine issue of material fact with respect to whether Microsoft's alleged nondiscriminatory reasons for firing the plaintiff were pretextual.[7] In *Harley v. McCoach*,[8] a female warehouse employee alleged that a hostile work environment was created by, among other incidents, an e-mail message addressing her as "Brown Sugar."[9] Even though the employer investigated her complaint and instituted remedial measures, the court denied its motion for summary judgment, finding that a genuine issue of material fact existed regarding whether the employer took prompt action upon learning about the hostile work environment.[10]

Some of these issues collide with employee privacy concerns, as employers seek to monitor their computer network to protect property, ensure proper use, and maintain a "quality product." Employees who feel that they have a right to privacy in their computer files have not received this type of monitoring well.

Controversy has long existed in the workplace, juxtaposing an employer's right to monitor its employees with an employee's right to privacy. This controversy has included issues dealing with providing company lockers,[11] monitoring phone calls,[12] and electronically monitoring performance.[13] Increased reliance on computers in the workplace is now resulting in employees claiming a right to privacy for work performed on computers, particularly e-mail.[14]

As most telecommuters rely heavily on electronic communications in performing their work, the outcome of this right to privacy issue will profoundly affect the practice of telecommuting. If an employer is not permitted access to employee computer files while the employee is absent from the office, the employer may decide to restrict, or entirely prohibit, telecommuting to limit potential liabilities. This Note discusses the use of telecommuting and the status of electronic communications law. Part II describes the present use of telecommuting, highlighting the advantages and the disadvantages. Part III analyzes current laws that affect electronic communications in the work environment. Part IV discusses key points required of new legislation to curb concerns over privacy rights regarding use of electronic communications in the workplace—points necessary to afford both the employer and the employee the requisite level of security.

II. Telecommuting and Its Increasing Use

Telecommuting can more specifically be defined as "periodic work outside of the central office, one or more days per week either at home or in a telework center" via computer or telephone.[15] As a result of substituting telecommunications technology for the daily commute to and from the primary workplace, telecommuters perform their work in a "virtual" office which, for example, can be either a home office, a telecommuting center,[16] a mobile office,[17] or a "hotelling" arrangement.[18] Thus, telecommuting can range from "simply working at home to the more complicated combination of flexiplace, flexitime, and electronic communications."[19] In 1996, an estimated 8.1 million workers were considered full-fledged telecommuters,[20] as they regularly connected to a corporate computer system via modem, while an additional 5.5 million workers intermittently used personal computers to work from the home or the road.[21] One consultant predicts that the number of telecommuters will grow to approximately 25 million by the year 2000.[22] Specifically, a significant increase in telecommuting can be anticipated in the next few years by the federal government, as the President's Management Council approved a National Telecommuting Initiative Action Plan in January 1996. This initiative calls for an increase from approximately 4000 federal telecommuters to 60,000 by year-end 1998 and 160,000 by year-end 2000.[23] Similar increases can be anticipated in the private sector as more companies discover the benefits that can result from instituting a telecommuting policy.

A. Advantages of Telecommuting

Flexible work benefits employers, employees, and society. From the employer's perspective, several specific benefits result from implementing a telecommuting program. Most readily apparent is an increase in employee productivity. While such results may be based partially on subjective assessments, many companies report productivity increases ranging from ten to forty percent.[24] Similar increases have been reported in positions such as data entry clerks, where gains may be objectively measured.[25] While some may believe these gains result from employees working longer hours, a better explanation may be that the home creates an environment more conducive to work. The employee is not subject to constant interruptions for quick questions or chats during the workday. Thus, the actual time spent working outside the formal workplace can produce a higher quality and quantity of work output.[26]

In addition to an increase in productivity, a decrease in absenteeism can be anticipated. Many absences occur due to an employee not being able to come to work for reasons including minor illnesses, emergencies, or personal appointments. A 1986 *Wall Street Journal* article estimated "that a day's absence of a clerical worker costs, in addition to wages, `up to 100 dollars in reduced efficiency and increased supervisory workload.'"[27] Considering the number of absences that occur in the workplace over the course of a year, these costs are far from trivial. When employees are able to perform some of their work from home, absenteeism decreases, thereby minimizing the total costs.[28] As the amount of time lost to absenteeism has doubled in the last ten years, this is a significant benefit.[29] Depending on the number of telecommuters in the workplace, the cost savings could be substantial. One researcher has estimated that telecommuters will take two less sick days per year.[30]

Recent examples of the use of telecommuting to reduce absenteeism include the Atlanta Olympics and recent California earthquakes. Operation Telecommute `96 was developed to provide relief to downtown Atlanta's workforce facing enormous traffic congestion during the games.[31] During the Olympics many commuters chose to telecommute instead of dealing with large crowds and long commutes each day.[32] During California's earthquakes in the early-to-mid 1990s, many companies established telecommuting arrangements and remote work centers for employees because conditions physically prevented or hindered travel to the corporate center.[33] With programs like these, work disruptions can be mitigated as companies quickly put plans into action.

Real estate and overhead costs will also be reduced as telecommuting becomes more popular. The estimated costs of a workstation range from $7000 for a public sector job and $10,000 to $15,000 for a private sector job.[34] Because each employee's workstation is not utilized one hundred percent of the time, the company can reduce the number of stations by combining those of telecommuters. For every workstation that is eliminated, the organization could realize annual savings of at least $5000—a substantial savings as the number of telecommuters increases.[35] One author suggests that a company can save two dollars for every dollar invested in telecommuting.[36]

Finally, telecommuting enables the employer to improve its retention of valuable employees as well as improve recruiting opportunities and results. The cost to recruit a new employee averages $8000, including direct recruiting costs, relocation expenses, personnel administration, and payroll costs.[37] The option of telecommuting creates incentives for employees to remain with the company and thereby increases the retention rate and decreases recruiting costs. At the same time, telecommuting allows the company to increase its base of potential employees, since the geographic location of available candidates greatly expands.[38]

Employees willing to telecommute will also share in the benefits. One of the most important benefits is a reduction in commuting time. This travel-time reduction may result in over two hundred hours saved annually—time which can then be spent on family, hobbies, and other activities.[39] Additionally, telecommuting offers greater flexibility in daily scheduling, including the arrangement of child and elder care, and the running of errands.[40] The reduced commuting also saves money and concurrently improves employees' mental health via reduced stress.[41]

With regard to the work itself, the employee is better able to communicate with his supervisor in some instances, as he can leave an e-mail message for the individual instead of participating in phone tag.[42] The employee may also be able to create a work schedule around the times he is most productive.[43] Additionally, the employee has more control over

working conditions (i.e., temperature or music), which make him more productive.[44] When an employee needs to focus on his current work, he can more easily channel "drop in" questions and discussions to particular times. As a result, the employee is able to work with fewer interruptions, which in turn also increases work productivity and reduces the work stress level.[45] Overall, telecommuting increases employee morale and job satisfaction; the employee is happy with his work conditions and feels more in control of his life.[46] Improved employee morale and job satisfaction translate to increased productivity for the employer and a higher return on personnel costs.[47]

Telecommuting also benefits society. Traffic congestion and air pollution are reduced as the number of employees physically traveling to their places of employment decreases. It is estimated that each driver could save two hundred gallons of gasoline and four quarts of oil each year by utilizing alternative work places.[48] As the number of traditional commuters decreases, more energy is conserved; traffic congestion lessens; the need for road repair reduces; and the need for public transportation diminishes.[49] In this way telecommuting also helps companies comply with federal and state environmental legislation such as the Clean Air Act.[50] For example, in a recent clean air campaign in Arizona, telecommuting was suggested as a way to reduce solo driving.[51] Additionally, telecommuting makes possible increased civic involvement in local communities as individuals have more free time available.[52]

B. Disadvantages of Telecommuting

Despite the many advantages of telecommuting, some disadvantages also exist. A major disadvantage for the employer is employee misperception of telecommuting.[53] Many employees view telecommuting as a substitute for costly daycare services or as a chance to be away from the office for a while; others think telecommuting will enable an employer to reduce staff needs and cause a lack of continuity in departmental communications.[54] Additionally, many managers fear they will lose direct control over the telecommuter's work, and as a result, the traditional style of management will not work with telecommuting.[55] Beyond the decrease in the direct control over employees, telecommuting reduces the number of face-to-face supervisory meetings; creates problems with off-site mechanical breakdowns; and decreases corporate flexibility in emergency situations.[56] Furthermore, only certain jobs are suitable for telecommuting, as some work must be done on company premises.

Planning can minimize many of these disadvantages. Employers must educate employees about telecommuting, and the benefits and opportunities it creates for them personally, as well as for the workplace. Without a change in management thinking, however, the barriers to telecommuting cannot be overcome. "Management must move from managing *attendance* to managing *performance*."[57] In a corporate environment where managers are constantly monitoring attendance (i.e., who is at his or her desk or worksite), telecommuting does not succeed. Managers do not feel comfortable with telecommuters, since their actual performance cannot be observed. However, when managers focus on results instead of attendance, telecommuting can thrive. Managers initiate this change in management style by trusting their employees to perform assigned work and then creating a system to monitor work progress and resolve the concerns of either party. Monitoring may include a shift in emphasis to meeting goals and deadlines for assignments, as well as periodic productivity checks. With the company's acceptance and proactive support, the manager can actually create a system that provides greater guidance for, and control over, employees through established communication procedures.[58]

For the employee, the main disadvantages of telecommuting include feelings of isolation and an inability to complete work tasks fully. Although the employee has chosen to work at home, feelings of isolation may occur since the employee no longer has daily contact with co-workers.[59] Employees may encounter different distractions that interfere with their work; alternatively, they may become workaholics. Additionally, the employee may have difficulty completing work assignments as they lack access to the necessary equipment (i.e., photocopier or fax machine).[60]

Proper planning and a well-developed telecommuting policy can help the telecommuter overcome many of these disadvantages.[61] For instance, the telecommuting employee should have a compatriot at the office to help alleviate feelings of isolation.[62] This person can provide necessary information from the office, as well as enabling the

telecommuter to stay in touch with office happenings. Finding the optimal mixture of an employee's time spent between home and workplace also may mitigate these problems.

For society, disadvantages include the potential loss of jobs and revenue.[63] For instance, the demand for bus drivers and toll collectors may decrease as fewer employees travel to work. Similarly, certain businesses, such as dry cleaners or restaurants, may lose business they have with traditional commuters. While some jobs may be lost as a result of telecommuting, its increasing use along with developing technology are certain to create new job opportunities to replace those lost.

III. Technology and the Law

Inasmuch as telecommuting definitions vary, it is difficult to accurately estimate the current number of telecommuters. Nevertheless, researchers estimate that telecommuting will continue to grow at an annual rate of fifteen to twenty percent.[64] As the information age continues,[65] and electronic communications use increases, telecommuters can perform more jobs. Presently, telecommuters are represented in every business or industry classification, with common occupations including salespersons, executives and managers, business professionals, technician/computer programmers, and teachers.[66]

A. Use of Technology

Advances in computer technology have greatly increased the work that can be done away from the office, and allow the telecommuter to remain in touch. Telecommuters can connect with the corporate office through Local Area Networks (LANs) allowing outside connections; Wide Area Networks (WANs) covering multiple offices; the Internet; or commercial online services.[67] Through the use of group software, telecommuters in different locations can access and work together on databases, documents, and spreadsheets.[68] Similarly, remote control software allows one computer to control another in a different location via a modem.[69] A telecommuter can then use any function from the remote computer that he would use if physically at the office, such as viewing, editing, and transferring files, or connecting with other workstations.[70] Additionally, an Integrated Services Digital Network (ISDN) allows a person to use one line to make both a voice and a computer call simultaneously. This structure enables employees at different sites to work together on documents and still talk to one another.[71]

On a basic level many companies have instituted an e-mail system. In a recent survey conducted by the Society for Human Resource Management, eighty-six percent of the respondents reported that their organizations used e-mail.[72] A 1997 Dun & Bradstreet study reported that e-mail usage by small businesses increased from sixteen to twenty-five percent in one year and that the trend was expected to continue.[73]

While e-mail in the workplace continues to grow, its use by businesses is not a new phenomenon. In a 1995 survey of 272 small to mid-size businesses, fifty-six percent reported use of e-mail within the company, forty-one percent exchanged e-mail with off site employees, twenty-three percent exchanged e-mail with suppliers, and eighteen percent exchanged e-mail with business advisors.[74] These companies also reported thirty-eight percent as having regularly telecommuting employees.[75] Already in 1995, eighty-seven percent of the *Fortune 100* companies reported using e-mail for person to person messaging.[76]

B. Protection of Electronic Communications Under the Law

Although e-mail systems in the workplace are common, the laws addressing employee privacy rights and employer monitoring rights are ambiguous. Currently, when employees connect to the company network, the access to and storage of files on the system may neither subject the employer to coverage under various laws, nor to liability under employee privacy claims. It is this uncertainty that may stunt the growth of electronic communications in the workplace and in turn telecommuting. Employers will limit the system's use to avoid potential liability. Employees seeking privacy will use other alternatives to communicate.

1. Electronic Communications Privacy Act of 1986

Congress adopted the Electronic Communications Privacy Act of 1986 (ECPA or Act)[77] to amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[78] commonly known as the federal wiretapping statutes. The purpose of the amendment was "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[79] Under the ECPA, unauthorized interception of electronic communications and unauthorized access to stored electronic communications are prohibited.[80] Electronic communications are defined under the Act as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . ."[81] While the ECPA does not directly discuss e-mail, the legislative history suggests it is generally within the scope of the Act.[82] As a result, electronic mail and computer-to-computer communications[83] are protected under the ECPA.[84] E-mail and computer files which are stored on a network would also be protected, since the ECPA protects unauthorized access to stored electronic communications as well.[85]

Clearly, the ECPA was enacted to provide greater privacy rights for individuals.[86] What remains unclear, however, is to what extent corporate computer systems are covered by the Act. Resulting coverage may affect the company's liability and, in turn, the use of telecommuting in general. Many corporate computer systems provide e-mail and computer-to-computer communications. Usually an employer's interception of or access to these electronic communications is intentional and thus would be a violation of the Act.[87] These violations could result in civil or criminal penalties for the employer.[88] However, three exceptions to the ECPA may limit its privacy protection for corporate employees.

a. Corporate System/Provider Exception

The first relevant exception exempts system providers from general ECPA prohibitions on both access and disclosure. Specifically, the Act provides:

> It shall not be unlawful under this chapter for . . . [an] officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . .[89]

One commentator has noted that public e-mail networks, such as Compu-Serve or MCI Mail, would most likely be included as "providers," while employers who subscribe to these networks for e-mail service may possibly be included as "agents."[90] Additionally, companies that provide their own e-mail systems on an interstate network may also be exempt as an electronic communications service provider.[91] Electronic communications service providers are also exempt from the broad prohibitions on accessing and disclosing electronically stored communications.[92] Electronic storage includes both the temporary storage of a message during transmission, as well as storage by the system provider for backup protection.[93]

Some commentators, including the Electronic Mail Association, interpret this exception as excluding private employers from liability for viewing and disclosing employee e-mail transmitted through company-owned computer systems.[94] Another commentator believes this exception further provides protection for an employer that monitors e-mail transmitted via a public service provider, as long as the service is used for internal communications only.[95] *Flanagan v. Epson America, Inc.*, an unpublished California Superior Court decision, provides support for these interpretations.[96] Although the case focused on the legality of e-mail interceptions under the California wiretapping statute, in a footnote the court discussed the applicability of the corporate system/provider exception under the ECPA and suggested that it would have exempted the employer/provider from liability.[97] Additionally, *Bohach v. City of*

Reno,[98] a district court decision, may provide further guidance. Here the court found that the city had acted lawfully when it accessed and retrieved stored electronic messages. The court considered the city to be a "provider" of electronic communications service, since it provided the terminals, computer, and software necessary for the users to send and receive electronic communications.[99] Thus, for employers with internal e-mail systems that do not rely on public service providers this exception may apply.

Legislative history also indicates that Congress did not intend to prohibit employers from viewing employees' electronic communications. The senate Report accompanying the passage of the Act recognized the existence of private internal e-mail systems, but did not address the expected effects the legislation would have on these particular systems.[100] Furthermore, during a Senate hearing much of the testimony on the proposed legislation reflected a concern for corporate privacy, rather than employee privacy.[101]

Other commentators warn employers against relying too heavily on this provision.[102] Legislative history also supports the opposite conclusion that employers are liable under the ECPA. Some testimony expressly acknowledged that the proposed legislation was intended to cover all electronic communications, including those on employer systems.[103] Supporters believed the Act should apply to all communications, since users "deserve privacy protection regardless of what type of entity runs their system."[104] Moreover, legislative history suggests the main purpose of this exception was to allow providers access to stored electronic communications in order to back-up messages in case of system failure.[105] This purpose is demonstrated by the inclusion of the language "for purposes of backup protection" within the definition of electronic storage.[106] Furthermore, as Congress specifically intended pre-ECPA prohibitions to continue applying to employers who intercept employee telephone conversations, it may not have had reason to expressly extend the prohibitions to electronic communications.[107] Additionally, as one commentator noted the intentions of Congress regarding e-mail regulation may be seen in its adoption of the strictest of three legislative options proposed in an Office of Technology Assessment report to Congress.[108] One of the goals of the option that Congress chose required it to pass legislation to "`[e]stablish the rights of the individual and responsibilities of the company when information is retained . . . .'"[109] This goal requires at the very least that employers inform employees of its policy regarding the "`uses and disclosure of personally identifiable information.'"[110]

Another factor which may influence coverage under the ECPA is an interstate commerce requirement. The Act requires electronic communications to be transmitted on a "system that affects interstate commerce."[111] The courts have yet to define the limits of this requirement. As the communication itself is not required to directly affect interstate commerce, a question arises as to the meaning of a system that "affects interstate commerce." Some communications made on systems are clearly covered, like the Internet and corporate computer systems linked over state lines. Other situations, such as an in-state employee connecting from home to the corporate system, are more ambiguous.[112] As a result, the ECPA may be interpreted as only protecting messages sent over public networks, such as the Internet, as these systems affect interstate commerce. However, one commentator noted that if the courts accept the legislative history suggesting Congress's intent to include protection of corporate internal systems, then a system may be protected by the ECPA even if an employer has no actual, physical presence in more than one state but its activities affect interstate commerce.[113] Thus, even companies with only internal systems may be found covered by the ECPA.

The applicability of this exception to employers remains unclear. Undoubtedly, the courts will decide the degree and manner of application to employers, particularly as numerous systems with various features are used. Even if the employer is found to be a provider or agent of a provider, it will still need to demonstrate that a particular interception was done in the ordinary course of business,[114] as well as demonstrating that the interception was necessary to render service or to protect its rights or property.[115] Prevention of system abuse, including computer crime and impermissible use, may provide a loophole through which employers can access telecommuters' accounts.

b. Business Exception

Another exception which may apply to employers is the business use exception. This provision has been relied on in telephone extension monitoring cases, but may not pertain to e-mail monitoring, unless telephone equipment or facilities are specifically involved.[116] The provision permits interceptions when telephone or telegraph equipment or components thereof are used in the ordinary course of business.[117] It remains to be seen whether courts will consider modems, computers, and software to be components of telephone equipment.[118]

In applying this exception to telephone extension monitoring cases, some courts have been fairly liberal in their interpretation. For example, in *Briggs v. American Air Filter Co.*,[119] the court held that monitoring was within the ordinary course of business when a supervisor monitored a business call in which an employee divulged trade secrets to a competitor.[120] In *James v. Newspaper Agency Corp.*,[121] the court held that a newspaper's telephone monitoring program for its telemarketing employees was squarely within the business use exception since it was conducted for a "legitimate business purpose" designed to help employees deal with the public effectively.[122]

Other courts, however, have limited the use of this exception according to the scope of the intrusion and the nature of the communication. For example, in *Watkins v. L.M. Berry & Co.*,[123] which involved an interception of a phone call, the court followed *Briggs*, but said it would only allow the unintentional interception of a personal call for a limited time, until the personal nature of the call was established.[124] Once the nature of the call is established as personal, any further monitoring would then be a violation of the ECPA.[125]

If courts are inclined to analogize e-mail interceptions to telephone extension monitoring, employers may be able to prove a legitimate business reason for e-mail monitoring, as long as it does not include reading the message in its entirety.[126] However, since even Congress has acknowledged that computer monitoring may be more difficult to implement than monitoring of telephone calls,[127] the courts may hesitate to do so. Nevertheless, courts may be willing to allow monitoring of electronic communications based on objective criteria (e.g., number of posts, receiver, sender, or elapsed time) rather than the actual content of the messages.[128] These results could then be used to determine if more intrusive monitoring is appropriate.[129] By using this type of monitoring, an employee's privacy is maintained while also providing an employer with a method of protecting its property.

Congress's intent for employers to monitor company computer systems may be evident in the Communications Decency Act of 1996 (CDA).[130] The CDA provides a defense for employers against the obscene or harassing use of telecommunications facilities by employees, unless the "employee's conduct is within the scope of employment and is known, authorized, or ratified by the employer."[131] This good faith defense can be used by employers when "`reasonable, effective and appropriate'" measures to restrict prohibited communications access are employed.[132] Thus, employers could argue that monitoring electronic communications is required to ensure that employees are not misusing the company system. Employers then will not be liable for any misuse that may occur. Furthermore, if an employee regularly engages in computer use as part of his work, a lack of monitoring may then signify the company's ratification of the employee's misuse of the system.

c. Consent Exception

The ECPA also allows for the interception or access of electronic communications where one of the parties to the communication has given prior consent.[133] In *Griggs-Ryan v. Connelly*,[134] the court found consent may either be express or implied. Implied consent could be inferred from surrounding circumstances indicating that the parties agreed to the surveillance.[135] However, courts do not construe the meaning of implied consent broadly.

In *Watkins v. L.M. Berry & Co.*,[136] the United States Court of Appeals for the Eleventh Circuit determined that an employee's knowledge of her employer's capability to monitor private phone calls could not be considered implied consent, even though the court found that Watkins had consented to a company policy allowing monitoring of phone calls for a limited time.[137] The court stated that the prior consent exception does not give the employer unlimited monitoring rights, but that it can be used to justify monitoring business calls, including the momentary interception of

personal calls until the personal nature of the call is established.[138] Thus, the monitoring of business communications and the inadvertent monitoring of personal communications may be allowed if the employer has a written policy addressing the issue.

In a working environment, this exception may be the best solution for all parties concerned. With an employee's consent, preferably express consent, the employer would be able to access e-mail messages as well as stored data. The employer should be leery of implied consent, as it could present a problem if the court interprets consent narrowly. Thus, it would be best to create an agreement where the employee gives express consent to the employer's access and monitoring each time he uses the electronic communications system.

2. State Legislation

In addition to federal legislation, many states have also adopted similar laws to protect an individual's right to privacy in electronic communications. Several states have enacted wiretap statutes that restrict the interception of wire communications. Many of these states have incorporated provisions of the ECPA, including the business use and prior consent exemptions.[139] Other states, however, offer greater protection to individuals by requiring prior consent of all parties to the communication.[140] These types of state laws would most likely not effect the use of electronic communications, even in telecommuting situations, because prior consent could be obtained in most circumstances. Because most communications in which the employer would be interested involve either the company, telecommuters, or other employees, consent from all employees would overcome this obstacle. When communications involve outside individuals such as clients, however, a problem may exist as consent from all parties is harder to achieve. Requiring an indication that any correspondence with the employer's e-mail address is monitored could resolve this problem.

Other states do not have statutes containing wiretapping provisions that may protect employees. For example, employers in Nebraska are specifically exempt under the state wire tapping provision.[141] A Nebraska employer is permitted "`on his, her, or its business premises . . . to intercept, disclose, or use [an electronic] communication in the normal course of his, her, or its employment.'"[142] While limiting the extent of monitoring permitted overall, the law authorizes monitoring "for mechanical, service quality, or performance control checks as long as reasonable notice of the policy of random monitoring is provided to their employees."[143]

Some states have proposed laws that "would specifically restrict the electronic monitoring practices of private" employers.[144] For example, a proposed law defeated in Texas "would have protected privacy by prohibiting secret electronic surveillance and unreasonable searches, and by preventing employers from obtaining unnecessary private information about employees."[145] Unfortunately, corporate lobbyists often pressure legislators to defeat such proposals.[146] Massachusetts corporations threatened to relocate to other states, successfully blocking similar legislation.[147] Past failures, though, have not stopped states from continually trying to pass legislation. For example, legislation proposed in Maryland during 1997 prohibited specified individuals from willfully intercepting electronic or wire communications sent and/or received by employees, or from willfully accessing or attempting to access an employee's computer, software, or database without the employee's authorization.[148] Similarly, a bill introduced in Connecticut in 1996 sought to prohibit an employer from monitoring the e-mail of employees without notification.[149]

Other states have successfully enacted legislation to account for changing technology.[150] Virginia, West Virginia, and Georgia have enacted similar laws addressing computer privacy.[151] The statutes make it illegal to use a computer (or network) to examine personal information without proper authority. A person is defined as being without authority if "he/she has no right or permission from the owner or has exceeded the scope of that right or permission."[152] Nevertheless, the effects these statutes may have on electronic communications remain unclear. For example, in the Virginia statute it is not clear whether the employer is considered the owner of the computer network and thus able to search the system that employees used for work-related activities.[153]

3. Invasion of Privacy Claims

As much of the federal and state law remains unclear about specific rights to e-mail privacy, many employees have turned to traditional methods to solve privacy disputes in the workplace—the common law or state privacy rights. In a recent case, *Smyth v. Pillsbury Co.*,[154] the court ruled a cause of action based on wrongful discharge did not exist when an employee claimed his termination was "in violation of `public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law.'"[155]

Smyth was an employee at Pillsbury Company, which maintained an e-mail system to promote internal corporate communications between employees. The company had repeatedly assured employees that all communications would remain confidential and privileged and that no communications could be intercepted and used by the company against the employee. Smyth, having received e-mail communications from his supervisor on his computer at home, relied on the company's assurances and responded to and exchanged messages with his supervisor. Later, the company intercepted the messages and notified Smyth that his employment was terminated for transmitting inappropriate and unprofessional comments over the company's e-mail system.

The court found Smyth did not have a reasonable expectation of privacy in the voluntary e-mail communications, notwithstanding the company assurances.[156] The court further stated that once an employee communicated the comments to a second person over the system which was used by the entire company, any reasonable expectation of privacy was lost.[157] Moreover, the court noted that even if a reasonable expectation of privacy did exist, the interception of the messages would not constitute a highly offensive invasion of privacy.[158] Finally, the court stated that "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."[159]

Although only at the district court level, this decision may predict the outcome of future common law claims. A common law tort for invasion of privacy generally occurs when "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to the reasonable person."[160] An employee may find this hard to prove, as the above case exemplifies. An employer has an interest in ensuring the proper use of the system to prevent any potential liability for employees' actions. As long as there is a legitimate reason (i.e. sabotage, loss of trade secrets, violation of business policy) for accessing an employee's electronic communications files, the intrusion most likely would not be considered highly offensive to a reasonable person. Furthermore, in a workplace setting, an employee should have no expectation of privacy in electronic communi
cations, for he uses the system to perform activities for the employer. Thus, an employee would rarely be able to prove the necessary elements for a claim of invasion of privacy.

In addition to common law claims, an employee may also be able to file a right to privacy claim. At least ten states have granted a constitutional right to privacy.[161] Since California courts have extended this privacy right to private actions,[162] many cases involving e-mail have been brought there. These cases provide a guide to the possible future success of such claims.

In *Flanagan v. Epson America Inc.*,[163] employees filed a civil class action suit against the company for invasion of privacy. The employees claimed that the company, without prior authorization, bypassed their passwords and read and printed all e-mail messages entering or leaving the company system, despite fostering an atmosphere of privacy regarding the messages.[164] Seven hundred employees used the company's e-mail system, which provided employee linkage via private password to approximately nine million computer terminals worldwide.[165] The court rejected the company's claim that the ECPA preempted the employees' state constitution-based privacy claim. Nevertheless, the court refused to find that the state right to privacy extended to employee e-mail; it preferred to leave this determination to the legislature.[166] In a companion case, *Shoars v. Epson America, Inc.*,[167] an employee brought a claim for invasion of privacy when she discovered that her supervisor was routinely reading and printing messages sent between the internal and external e-mail services. The employee was fired after she allegedly opened a private account for personal messages.[168] The court dismissed her invasion of privacy claim as well.[169]

The California court also dismissed the employees' invasion of privacy claims in *Bourke v. Nissan Motor Co.*[170] Here, the plaintiffs were two employees hired to set up and run an e-mail system between Nissan and its Infiniti dealers. The employees had received final warnings after their supervisor printed out their messages and found some inappropriate jokes and language. The employees complained about the monitoring and were eventually fired. Nissan successfully argued that the employees had no reasonable expectation of privacy in their messages, as they had signed a computer registration form containing the company policy restricting the system to business use only.[171]

IV. Need for New Legislation

The need for new legislation to remove existing ambiguities is apparent. Employees currently have no assurance of privacy rights in all employment settings and employers currently have no assurance of privacy for their computer networks. Factors such as the employer's location and the type of communications system provided determine specific, often unique, rights. As a result, the battle between employers' interest in monitoring business and employees' concerns for privacy continues as each believes the law is on his side. A solution is necessary in order to encourage employers to take full advantage of advances available in communications and computer technologies and the resultant benefits, such as telecommuting.

In formulating this solution, a federal response is most desirable, as it will establish a uniform policy. Federal legislation would apply not only to interoffice electronic communications but also to interstate communications, thereby eliminating any discrepancies that may exist in employer coverage. Corporate lobbyists would have less influence as threats of relocating corporations will no longer be significant, since the law will apply everywhere.[172]

Federal legislation should be simple and broad so as to cover all of the various workplace situations. Coverage of the provision would include all employers that use electronic communications in the workplace. As a result, the problems encountered with the Electronic Communications Privacy Act would be eliminated, since all employers would be uniformly covered. The legislation should require employers to have a legitimate business purpose when accessing employee accounts, limitations should be placed on access to and use of information found, and reasonable notice should be provided to employees as to when monitoring may occur.

Additionally, the provision should require that employers provide all employees using an electronic communications system with a company policy specifically outlining how the above objectives are to be accomplished. This policy should include a statement specifying that the system is for business purposes only. If personal use of the system is permitted, the extent of such use should also be explicitly defined. Moreover, since no system is completely secure, employees should be forewarned and instructed not to transmit any confidential material or other information that they or their employer would not want known to others. The business purposes that the employer may have for accessing employee computer accounts should also be noted. These purposes may include accessing work files located in a telecommuter's account on a telecommuting day, randomly checking
adherence to the company's no personal use policy, or investigating complaints about messages sent to certain employees. For each of the these stated business purposes, the employer should specify the notice it will provide to the employee and the limitations placed on use of the information collected, ideally restricting it to the stated purpose.

Additional necessary provisions also include procedures the employer intends to follow when accessing employee accounts and a listing of the individuals who have access to these accounts. Furthermore, procedures for employees to file complaints about access they deem inappropriate under the policy should exist. Ideally, an individual who is not authorized to access another employee's account (e.g., human resources department) should be in charge of this procedure to provide an impartial decision regarding the access. This would then provide the employee some degree of comfort, as he knows that access is not automatic. This system should also provide checks and balances on managers, supervisors, and others who may access accounts. For instance, managers should regularly review a supervisor's computer activities for improper access to employee files. Finally, if a policy includes random checks, accounts must be monitored on a regular basis. Therefore, individuals who are caught in violation of the policy cannot argue that they are being targeted.

Keeping the policy fairly broad provides greater flexibility, which allows the legislation to cover the various types of

electronic communications commonly used in the business environment. This proposed legislation provides a balance between the employee's right to privacy and the employer's right to conduct business. The employee will choose the level of privacy desired in making his employment decision. For instance, an employee may be willing to give up some degree of privacy in exchange for the ability to telecommute. An employee will know that communicating electronically with outside parties may be subject to review, whereas inside communications may not. Thus, in using electronic communications the employee will be aware of the level of privacy to expect and will have recourse if this expectation is violated. The employer can then monitor electronic communications to protect its business interest, as long as the policy is followed.

V. Conclusion

Without new legislation, the benefits of electronic communications in the workplace, such as telecommuting, will remain significantly underutilized. Only legislation that acknowledges an employer's right to access employees' computer accounts and unilaterally retrieve information while concurrently providing employees with some degree of privacy in their communications will end the current privacy debate. These issues do not represent diametrically opposed goals. Once employers realize they legally have access to monitor the corporate computer system to protect their property, they will feel more comfortable in allowing employees to work away from the office. Once employees realize they have a certain degree of privacy in their electronic communications, they will feel more comfortable in choosing telecommuting options. As a result, the employer, employee, and society could experience the many benefits of telecommuting.

* B.S., Purdue University Calumet, 1993; candidate for J.D., Indiana University School of Law—Bloomington, 1998.

1. Jack Nilles, *Some Common—and Not So Common—Telework/Telecommuting Questions and Jack Nilles's Answers and Comments* (visited Jan. 29, 1998) <http://www.jala.com/faq.htm>.

2. *U.S. Telecommuting Trend Surpasses 11 Million* (visited Feb. 1, 1998) <http://etrg.findsvp.com/prls/pr97/telecomm.html>.

3. *See infra* Part III.A.

4. Roger Martin, *Small Business: Electronic Mail Opens New World of Privacy Issues for Employers*, Det. News, Nov. 11, 1996, at F8.

5. *Morgan Stanley Hit by E-Mail Lawsuit*, Telecomworldwire, Jan. 31, 1997.

6. *Strauss*, 814 F. Supp. 1186 (S.D.N.Y. 1993).

7. *Id.* at 1194.

8. *Harley*, 928 F. Supp. 533 (E.D. Pa. 1996).

9. *Id*. at 537.

10. *Id.* at 537, 540.

11. *See* K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. App.—Houston [1st Dist.] 1984, writ ref'd n.r.e.) (holding that an employee possessed a reasonable expectation of privacy in a locker secured with her own lock).

12. *See* Briggs v. American Air Filter Co., 630 F.2d 414 (5th Cir. 1980) (discussing the legality of an employer listening to employee phone calls).

13. *See* Office of Tech. Assessment, The Electronic Supervisor: New Technology, New Tensions (1987) (discussing electronic monitoring in the workplace).

14. *See infra* Part III.B.3.

15. Nilles, *supra* note 1.

16. A telecommuting center is a facility that provides an alternative site other than the corporate office for employees to perform work activities. 1995 U.S. Gen. Servs. Admin., Interim Report: Federal Interagency Telecommuting Centers (1995), *reprinted at* <http://tsd.r3.gsa.gov/tcommute/ir_fitc.htm>; Alice Bredin, The Virtual Office Survival Handbook 7 (1996).

17. This term is used by individuals who spend a lot of time traveling and describes, for example, a car or a briefcase. These individuals have the necessary technology to perform their work from such an "office" without needing to return to the corporate office. Bredin, *supra* note 16, at 8.

18. Hotelling is a term coined by Ernst & Young, LLP, to describe its program in which employees make work arrangements to use desks or other company work space on an as-needed basis. *Id.* at 8-9.

19. George M. Piskurich, *Making Telecommuting Work*, Training & Dev., Feb. 1996, at 20, 23.

20. Meg Fletcher, *Doing Your Homework*, Bus. Ins., Apr. 15, 1996, at 22, 22.

21. *Id.*

22. Nilles, *supra* note 1.

23. Memorandum from the President's Management Council Working Group on Telecommuting to the Executive Department and Agency Heads (Feb. 22, 1996), *reprinted at* <http://tsd.r3.gsa.gov/tcommute/act2mem.htm>; Andrew Zajac, *Telecommuting from Home Becomes Reality for Millions* (visited Feb. 1, 1998)

<http://www.nando.net/newsroom/ntn/info/101997/info10_26956_noframes.html>.

24. Debra Schepp & Brad Schepp, The Telecommuter's Handbook 7 (2d ed. 1995).

25. Joel Kugelmass, Telecommuting: A Manager's Guide to Flexible Work Arrangements 51-52 (1995).

26. *Id.* at 53-54.

27. *Id.* at 55 (quoting Selwyn Feinstein, *A Special News Report on People and Their Jobs in Offices*, Wall St. J., July 29, 1986).

28. Kugelmass, *supra* note 25, at 55-56.

29. *Id.* at 55.

30. Jack M. Nilles, Making Telecommuting Happen 140 (1994).

31. *`96 Summer Games Set Vigorous Telecommuting Trend in Atlanta*, Can. Newswire Ltd., Sept. 5, 1996, *available in* WestLaw, Canadanews File.

32. Merlisa Lawrence Corbett, *Telecommuting: The New Workplace Trend*, Black Enter., June 1996, at 256, 258.

33. Kugelmass, *supra* note 25, at 61-62; Gary Fisher, *Downhill and Cross Country*, Elec. Eng'g Times, Oct. 30, 1995, at 84.

34. *Telecommute America—Benefits* (visited Feb. 21, 1998)

<http://tsd.r3.gsa.gov/buttonmap.map?44,36>. Another author has noted that savings on real estate costs alone can total between $1500 and $5000 per year. Kim Girard, *ComputerWorld Forecast 98*, ComputerWorld, Jan. 5, 1998, at 31.

35. *Telecommute America—Benefits*, *supra* note 34.

36. Piskurich, *supra* note 19, at 22.

37. *Telecommute America—Benefits*, *supra* note 34.

38. Kugelmass, *supra* note 25, at 60.

39. *Telecommute America—Benefits*, *supra* note 34.

40. Piskurich, *supra* note 19, at 22.

41. *Id.*

42. *Id.*

43. Kugelmass, *supra* note 25, at 59-60; Piskurich, *supra* note 19, at 22.

44. Piskurich, *supra* note 19, at 22.

45. *Id.*

46. Kugelmass, *supra* note 25, at 58-59.

47. *Id.*

48. *Telecommute America—Benefits*, *supra* note 34. AT&T estimates that its 36,000 teleworkers will have reduced carbon dioxide emissions by 80,000 tons in 1997. *AT&T Survey Reveals Boomers Taking Control of Their Lives Through Telework*, M2 Presswire, Oct. 21, 1997, *available in* 1997 WL 15140080 [hereinafter *AT&T Survey*].

49. Piskurich, *supra* note 19, at 22.

50. John Menchen, *Insurers Lead Way in Growth of Telecommuting*, Nat'l Underwriter (Property & Casualty Risk & Benefits Mgmt. Ed.), Aug. 12, 1996, 25, 27.

51. Mary Jo Pitzl, *More Get `Don't Drive' Message*, Ariz. Republic, Nov. 17, 1997, at B1.

52. U.S. Gen. Servs. Admin., *supra* note 16, at 13.

53. Piskurich, *supra* note 19, at 22.

54. *Id.* at 22-23.

55. Corbett, *supra* note 32, at 260.

56. Piskurich, *supra* note 19, at 23.

57. David Chaudron, *The "Far Out" Success of Teleworking*, Supervisory Mgmt., Jan. 1995, at 1, 6.

58. *See* Corbett, *supra* note 32, at 260.

59. *Id.* at 258. A recent survey of telecommuters found, however, that 62% of respondents did not feel a difference when working at home and 15% of respondents felt more connected at home than at work. Only 20% of respondents reported increased feelings of isolation. *AT&T Survey*, *supra* note 48.

60. Piskurich, *supra* note 19, at 23.

61. For a brief description of Merrill Lynch's telecommuting training program see, Kirk Johnson, *Limits on the Work-at-Home Life*, N.Y. Times, Dec. 17, 1997, at B1.

62. Schepp & Schepp, *supra* note 24, at 32.

63. Piskurich, *supra* note 19, at 20, 23.

64. Schepp & Schepp, *supra* note 24, at 3; Motorola, *Working at Home Has Never Been so Easy* (visited Jan. 29, 1998) <http://www.mcu.motsps.com/bu/mctg/office.html>; Nilles, *supra* note 1.

65. A rapidly expanding part of the economy is the service sector, in which employment is expected to grow at 3% per year until 2005, while the manufacturing sector is expected to decline at .7% per year. Bureau of the Census, U.S. Dep't of Commerce, Statistical Abstract of the United States 411 (116th ed. 1996).

66. *AT&T Survey*, *supra* note 48.

67. Elana N. Broder, Note, *(Net)workers' Rights: The NLRA and Employee Electronic Communications*, 105 Yale L.J. 1639, 1640 (1996); *see* Paula Ancona, *Tips for Telecommuters*, Ariz. Republic, Mar. 6, 1995, at E4.

68. Broder, *supra* note 67, at 1645.

69. Ancona, *supra* note 67.

70. *Id.*

71. Francy Blackwood, *Paving the Way*, S.F. Bus. Times, Dec. 20, 1996, at A20.

72. *E-Mail Training and Policy Helps Employers Avoid Accidents Along Information Highway*, PR Newswire, Nov. 20, 1997, *available in* LEXIS, News Library; PRNews File.

73. John Long, *Chatting up the Net*, VARBusiness, Nov. 1, 1997, *available in* 1997 WL 7700277.

74. *Interoffice E-mail*, Inc., Sept. 1995, at 116, 116 (discussing the results of a survey conducted by the Executive Committee, San Diego, April 1995).

75. *Id.*

76. *Keeping in Touch*, USA Today, Mar. 1, 1995, at 1B.

77. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at scattered sections of 18 U.S.C. (1994)).

78. 18 U.S.C. §§ 2510-20 (1994).

79. S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

80. *See* 18 U.S.C. §§ 2511(1)(a), 2701(a).

81. *Id.* § 2510(12).

82. S. Rep. No. 99-541, at 14, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

83. Computer-to-computer communications "include . . . the transmission of proprietary data among the various offices of a com
pany." *Id.* at 8, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562.

84. *Id.* at 14, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

85. 18 U.S.C. §§ 2701, 2711.

86. S. Rep. No. 99-541, at 1-2, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-56.

87. *See id.* at 23, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

88. 18 U.S.C. § 2511(4)(a).

89. *Id.* § 2511(2)(a)(i).

90. Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"*, 28 J. Marshall L. Rev. 139, 156 (1994).

91. *Id.*

92. 18 U.S.C. § 2701(c)(1).

93. *Id.* § 2510(17); *see also* S. Rep. No. 99-541, at 35 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589.

94. Larry O. N. Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 Harv. J.L. & Tech. 345, 359 (1995); Julia Turner Baumhart, Note, *The Employer's Right To Read Employee E-Mail: Protecting Property or Personal Prying?*, 8 Lab. Law. 923, 925 (1992).

95. Gantt, *supra* note 94, at 360.

96. *Id.* at 360 & n.99 (citing Flanagan v. Epson Am., Inc. (Sup. Ct. Cal. Jan. 4, 1991 (unreported)).

97. *Id.* at 360 & n.100.

98. *Bohach*, 932 F. Supp. 1232 (D. Nev. 1996).

99. *Id*. at 1236.

100. Baumhart, *supra* note 94, at 926 (analyzing S. Rep. No. 99-541, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562).

101. *Id.*

102. Gantt, *supra* note 94, at 360 & n.101.

103. *Electronic Communications Privacy Act: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary*, 99th Cong., 99-100 (1985) (prepared statement of Philip M. Walker, Vice Chairman of the Electronic Mail Ass'n.); *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Comm. on the Judiciary*, 99th Cong. 21 (1986) (testimony of Philip M. Walker, Vice Chairman of the Electronic Mail Ass'n) [hereinafter *Hearing on H.R. 3378*].

104. *Hearings on H.R. 3378* (testimony of Philip M. Walker, Vice Chairman of the Electronic Mail Ass'n), *supra* note 103.

105. Baumhart, *supra* note 94, at 928. "E-mail systems are designed to provide access to contents and copies of messages in case of system failure. Messages are electronically generated and not normally accessed by the e-mail provider." H. Rep. No. 99-647, at 22 n.34 (1986).

106. 18 U.S.C. § 2510(17)(B) (1994).

107. Baumhart, *supra* note 94, at 927.

108. *Id.* at 928. For a listing of the three options proposed, see Office of Tech. Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties 51-52 (1985).

109. Baumhart, *supra* note 94, at 928 (quoting Office of Tech. Assessment, *supra* note 108, at 51).

110. *Id.*

111. 18 U.S.C. § 2510(12); *see also* S. Rep. No. 99-541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3565-66.

112. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 91 (1994).

113. *Id*.

114. Lee, *supra* note 90, at 156.

115. 18 U.S.C. § 2511(2)(a)(i).

116. Lee, *supra* note 90, at 155.

117. 18 U.S.C. § 2510(5)(a).

118. Lee, *supra* note 90, at 155.

119. *Briggs*, 455 F. Supp. 179 (N.D. Ga. 1978), *aff'd*, 630 F.2d 414 (5th Cir. 1980).

120. *Id.* at 181.

121. *James*, 591 F.2d 579 (10th Cir. 1979).

122. *Id.* at 581-82.

123. *Watkins*, 704 F.2d 577 (11th Cir. 1983).

124. *Id.* at 581-82.

125. *Id.* at 584.

126. Lee, *supra* note 90, at 156.

127. "It is impossible to `listen' to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation." S. Rep. No. 99-541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585. While discussing the minimization of interceptions, Congress noted that "computer transmissions would require a somewhat different procedure than that used to minimize a telephone call." *Id*.

128. Baumhart, *supra* note 94, at 933.

129. *Id.*

130. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified in scattered sections of 47 U.S.C.A. (West Supp.)).

131. H.R. Conf. Rep. No. 104-458, at 188 (1996), *reprinted in* 1996 U.S.C.C.A.N. 124, 201.

132. *Id.*

133. 18 U.S.C. §§ 2511(2)(d), 2701(c)(2) (1994).

134. *Griggs-Ryan*, 727 F. Supp. 683 (D. Me. 1989), *aff'd sub nom.* Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990).

135. *Id.* at 686.

136. *Watkins*, 704 F.2d 577 (11th Cir. 1983).

137. *Id.* at 581.

138. *Id.* at 581-82.

139. *See* Paul E. Hash & Christina M. Ibrahim, *E-Mail, Electronic Monitoring and Employee Privacy*, 37 S. Tex. L. Rev. 893, 904 & n.81 (1996) (listing states which have both exemptions). These states are: Arizona, Colorado, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Iowa, Kansas, Louisiana, Maryland, Minnesota, Mississippi, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Texas, Utah, Virginia, West Virginia, Wisconsin, and Wyoming.

140. *Id.* at 904-05.

141. *Id.* at 905.

142. *Id*. (quoting Neb. Rev. Stat. § 86-702(2)(a) (1994)).

143. Neb. Rev. Stat. § 86-702(2)(a) (1994).

144. Hash & Ibrahim, *supra* note 139, at 905.

145. Lee, *supra* note 90, at 160 (citing Terry M. Dworkin, *Protecting Private Employees from Enhanced Monitoring: Legislative Approaches*, 28 Am. Bus. L.J. 59, 81 (1990)).

146. *Id.*

147. Gantt, *supra* note 94, at 411.

148. H.B. 542, 1st Reg. Sess. (Md. 1997).

149. H.B. 6623, 1st Reg. Sess. (Conn. 1997).

150. Jill L. Rosenberg, *Legal Issues Surrounding Employee Hiring, Privacy and Investigations*, 547 PLI/Lit 569, 631 (1996).

151. *Id.* (citing Va. Code § 18.2-152; Ga. Code Ann. § 16-9-90; W. Va. Code § 61-3C-1).

152. *Id.* at 631-32.

153. *Id.*

154. *Smyth*, 914 F. Supp. 97 (E.D. Pa. 1996).

155. *Id.* at 100 (quoting Complaint at &15).

156. *Id.* at 101.

157. *Id.*

158. *Id.*

159. *Id.*

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

161. Baumhart, *supra* note 94, at 943 & n.124; Frank C. Morris, Jr., *E-Mail Communications: The Next Employment Law Nightmare*, 20 A.L.I-A.B.A., Dec. 1995, at 49, 51 (listing the following states that grant their citizens a constitutional right to privacy: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Missouri, South Carolina, and Washington).

162. Steven L. Willborn et al., Employment Law: Cases and Materials 189 (1993).

163. Hash & Ibrahim, *supra* note 139, at 906 (citing Flanagan v. Epson Am., Inc. (Sup. Ct. Cal. Jan. 4, 1991 (unreported)); Morris, *supra* note 161, at 56 (discussing Flanagan v. Epson Am., Inc.).

164. Hash & Ibrahim, *supra* note 139, at 906.

165. *Id.*

166. *Id.*

167. *Id.* (citing Shoars v. Epson Am., Inc. (Cal. Ct. App.) (unreported), *rev. denied*, No. S040065, 1994 Cal. LEXIS 3670 (Cal. June 29, 1994)); Morris, *supra* note 161, at 56 (discussing Shoars v. Epson Am., Inc.).

168. Hash & Ibrahim, *supra* note 139, at 906.

169. *Id.* at 906-07.

170. *Id.* (citing Bourke v. Nissan Motor Co. (Sup. Ct. Cal. 1991) (unreported)). The California Court of Appeals, Second Appellate District, affirmed the Superior Court=s decision. *See id.* at 907 & n.93.

171. *Id.* at 907.

172. *See supra* text accompanying note 145.