Computer technology and the Internet have become indispensable assets in the workplace. However, courts and legislatures are one step behind in interpreting and creating laws that will adequately reflect the interaction between this new technology and society. As a result of this absence of clear legislation and judicial precedent, it is difficult to advise a client as to the implementation of computer and Internet policies. The prudent lawyer should, therefore, formulate and recommend a computer and Internet policy that accounts for all reasonably foreseeable interpretations of the law.

One growing area of concern is the issue of employee privacy in the computer age. Employees commonly engage in computer and Internet-related activities in the workplace, and the majority of these activities are conducted on computer systems owned and operated by the employer. Electronic communications are routinely sent, received and stored with the aid of employer computer systems and electronic documents are routinely stored in these systems. This begs the question of whether an employee has a privacy interest in any of these communications or documents and, if so, what the nature and the scope of that privacy interest is. Confusing matters, is the case of employees who are telecommuting, especially when they are using company-owned computers.

There are currently four main sources of law relevant to the “electronic privacy” of employees. First, is a common law tort for the “unreasonable intrusion on the seclusion of another.” Second, a constitutional action is available to public employees under the search and seizure provisions of the Fourth Amendment of the U.S. Constitution. Third, there are statutory causes of action under both federal and New Jersey law. Finally, there may be statutes that create a property interest in electronic data which are relevant to an employer’s ability to delete employee e-mails, electronic documents and other data files. New Jersey, for example, has two such statute. The first part of this article explores these applicable sources of law and suggests protocol that employers may wish to implement to prevent and avoid liability for monitoring, viewing, taking or erasing electronic communications, documents or data in the workplace. The second part will address student privacy issues.

Part I: Employee Privacy Interests
Common Law Tort Actions

Those who offend the privacy interest of another may be held liable in tort for an “unreasonable intrusion upon another’s seclusion.” An “unreasonable intrusion” is measured from the standard of what a reasonable person would find “highly offensive,” and the tort consists of an intentional intrusion into the “private affairs or concerns” of another. The law does not demand that the intrusion be physically perpetrated, and a cause of action may properly
The intrusion must be both objectively and subjectively unreasonable for the claim to be properly brought.\(^6\)

arise out of “the use of the defendant’s senses to oversee or overhear the plaintiff’s private affairs” in an investigation or examination.” An arguably unreasonable intrusion will not form the basis of liability if the employee had consented to the intrusion.

The intrusion must be both objectively and subjectively unreasonable for the claim to be properly brought.\(^6\) There is generally a lowered employee expectation of privacy in the workplace, and furthermore, there can be no expectation of privacy if an employee conducts the activity in a manner “open” to other employees. One federal district court (applying Pennsylvania law) has held that there is no recognizable privacy interest in employee e-mails, even when middle management has guaranteed that employee e-mails would remain confidential.\(^9\) Presumably, if an employee is working at home, his or her expectation of privacy would be greater than if at the office, and greater still if the employee were working on his or her own computer.

In the event that the employer is a public employer, a damages claim for an unreasonable intrusion upon another’s seclusion may be greatly limited by state legislation. Many states have enacted legislation comparable to the Federal Torts Claim Act which greatly reduces the tort liability of state actors.\(^10\) For example, the New Jersey Tort Claims Act places a severe limit on damage recoveries for pain and suffering. The federal court for the district of New Jersey has interpreted this to limit emotional distress damages that flow from a tortious intrusion on one’s seclusion.

Constitutional Actions

A civil action may also be brought under the search and seizure provisions of the Fourth Amendment to the US. Constitution if a public employer commits an intrusion on an employee’s privacy.” These suits are often brought as a Section 1983 claim for damages.\(^13\) One relevant question that has arisen in this area is what exactly constitutes the scope of a “workplace” for the purpose of the Fourth Amendment right to privacy.\(^24\) O’Connor v. Ortega, the U.S. Supreme Court attempted to answer this question through the use of a “luggage” analogy.\(^4\)

First, the Court articulated that the workplace consists of all facilities and physical premises, including personal workplace office, desk, and filing cabinets of an employee.” The Court continued by discussing a hypothetical situation in which an employee brings a piece of personal luggage to the workplace. Although the outward appearance of the luggage may be subject to the diminished expectation of privacy, the contents of such luggage are not. How this analogy may be applied to the electronic context has yet to be seen.

The Ortega Court continued by stating that employees do not automatically lose their expectation of privacy simply because they are in the workplace.\(^8\) The reasonableness of a workplace privacy expectation may be ascertained by looking to the relationship between the employer and the employee.\(^17\) As a result, the workplace expectation of privacy must be addressed on a case-by-case basis.” The Court found that a public-hospital doctor may have a reasonable expectation of privacy in the contents of his personal workplace office under some circumstances.\(^19\)

The Court then stated that even in the presence of a reasonable expectation of privacy, a public employer might still conduct reasonable searches.\(^30\) A public employer has an interest in “the efficient and proper operation of the workplace” that must be balanced against the employee’s right to privacy.\(^26\) Public employer intrusions on employee privacy may be held reasonable if they are for either: (1) “noninvestigatory, work-related purposes,” or (2) investigations of work-related misconduct.\(^27\) Finally, it should be noted that the privacy intrusion must be justified both at its inception and in its scope.\(^23\)

As an additional matter, it should be noted that the New Jersey Constitution also provides for a right to privacy.\(^24\) It has been held that the search and seizure provisions of the New Jersey Constitution create a limited right to be free from government intrusions into private affairs.\(^25\) The New Jersey Supreme Court has also indicated that the violation of the right of privacy by a private employer may form the basis of a wrongful discharge suit if the discharge was based on a violation of the employee’s privacy interest.\(^26\)

Federal and State Statutory Actions

The federal Electronic Communications Privacy Act (ECPA) is another source of employer liability for an intrusion on the electronic privacy of another.\(^1\) The ECPA provides for both civil and criminal liability, and it is divided into two titles. Title I deals with the unauthorized and intentional interception of transitory electronic communications,\(^28\) and Title II deals with intentionally gaining access to stored communications without authorization.\(^29\)

In general, Title I of the ECPA prohibits: (1) intentional interceptions of transitory electronic communications, and (2) intentional uses or disclosures of content procured by interceptions of transitory electronic communications.\(^30\) There are two important exceptions to ECPA’s prohibition on intentional interceptions: (1) the “business use exception,” and (2) the “consent exception.”

The business use exception permits intentional and unauthorized interceptions if the interceptions are “within the regular course of business” and if the employer has a “legal interest” in the subject matter of the communication.\(^27\) Although an employer may monitor business communications, the scope of the exception does not include personal communications. For example, and by analogy, one court has held that when an employee uses an employer’s phone to conduct a job interview with a potentially new employer, such a conversation may not be monitored.

Constitutional Actions

A civil action may also be brought under the search and seizure provisions of the Fourth Amendment to the US. Constitution if a public employer commits an intrusion on an employee’s privacy.” These suits are often brought as a Section 1983 claim for damages.\(^13\) One relevant question that has arisen in this area is what exactly constitutes the scope of a “workplace” for the purpose of the Fourth Amendment right to privacy.\(^24\) O’Connor v. Ortega, the U.S. Supreme Court attempted to answer this question through the use of a “luggage” analogy.\(^4\)

First, the Court articulated that the workplace consists of all facilities and physical premises, including personal workplace office, desk, and filing cabinets of an employee.” The Court continued by discussing a hypothetical situation in which an employee brings a piece of personal luggage to the workplace. Although the outward appearance of the luggage may be subject to the diminished expectation of privacy, the contents of such luggage are not. How this analogy may be applied to the electronic context has yet to be seen.

The Ortega Court continued by stating that employees do not automatically lose their expectation of privacy simply because they are in the workplace.\(^8\) The reasonableness of a workplace privacy expectation may be ascertained by looking to the relationship between the employer and the employee.\(^17\) As a result, the workplace expectation of privacy must be addressed on a case-by-case basis.” The Court found that a public-hospital doctor may have a reasonable expectation of privacy in the contents of his personal workplace office under some circumstances.\(^19\)

The Court then stated that even in the presence of a reasonable expectation of privacy, a public employer might still conduct reasonable searches.\(^30\) A public employer has an interest in “the efficient and proper operation of the workplace” that must be balanced against the employee’s right to privacy.\(^26\) Public employer intrusions on employee privacy may be held reasonable if they are for either: (1) “noninvestigatory, work-related purposes,” or (2) investigations of work-related misconduct.\(^27\) Finally, it should be noted that the privacy intrusion must be justified both at its inception and in its scope.\(^23\)

As an additional matter, it should be noted that the New Jersey Constitution also provides for a right to privacy.\(^24\) It has been held that the search and seizure provisions of the New Jersey Constitution create a limited right to be free from government intrusions into private affairs.\(^25\) The New Jersey Supreme Court has also indicated that the violation of the right of privacy by a private employer may form the basis of a wrongful discharge suit if the discharge was based on a violation of the employee’s privacy interest.\(^26\)

Federal and State Statutory Actions

The federal Electronic Communications Privacy Act (ECPA) is another source of employer liability for an intrusion on the electronic privacy of another.\(^1\) The ECPA provides for both civil and criminal liability, and it is divided into two titles. Title I deals with the unauthorized and intentional interception of transitory electronic communications,\(^28\) and Title II deals with intentionally gaining access to stored communications without authorization.\(^29\)

In general, Title I of the ECPA prohibits: (1) intentional interceptions of transitory electronic communications, and (2) intentional uses or disclosures of content procured by interceptions of transitory electronic communications.\(^30\) There are two important exceptions to ECPA’s prohibition on intentional interceptions: (1) the “business use exception,” and (2) the “consent exception.”

The business use exception permits intentional and unauthorized interceptions if the interceptions are “within the regular course of business” and if the employer has a “legal interest” in the subject matter of the communication.\(^27\) Although an employer may monitor business communications, the scope of the exception does not include personal communications. For example, and by analogy, one court has held that when an employee uses an employer’s phone to conduct a job interview with a potentially new employer, such a conversation may not be monitored.
because it is not within the regular course of business." On the other hand, a court has found a telephone call to be within the regular course of business: (1) when the call was between employees; (2) when the call was made during office hours; and (3) when the remarks were about a supervisor. Similarly, it has been held that an employer may monitor an employee's phone conversation when the employer suspects that the employee is revealing confidential trade secrets and the monitoring is limited in time and purpose.34

If an employer would like to possess the legal ability to continually monitor all electronic communications, it is advisable for the employer to articulate such a policy in writing and define the exact nature and scope of the monitoring process. Again, by analogy, one court has held that a policy of monitoring all telephone calls constitutes a monitoring within the ordinary course of business, provided that all employees were aware that the phones would be monitored for "quality control."35 As such, all written policies should he distributed to all employees.

The consent exception permits intentional interceptions when there has been express or implied consent.36 This exception requires that an employer give notice of monitoring to employees in order to avoid liability. One court held that notice need not be formal, but it should be "more than casual" and should communicate the fall scope of the monitoring." Another court has held that notice by itself is not enough and that assent may be required.37 Finally, it is important to note that the element of consent is satisfied even if only one party to the communication has consented.38

Title II of the ECPA provides for civil and criminal liability for the intentional and unauthorized access to stored electronic communications.40 Even if an employer does not have the right to "intercept" an electronic message, the employer may still be able to access the message once it is in electronic storage. However, the extent to which an employer may be able to monitor stored employee communications under the ECPA will depend largely on the judicial interpretation of the term, "authorized." For example, a court may or may not find that employee authorization is implicit since the employee is obviously aware that the communications are being stored on the employer's own computer.

When reading Title I and Title II of ECPA together, the question arises: Does an unopened e-mail constitute a transitory communication or a stored communication? The difference is significant, because statutory damages for stored communications are $1,000 per violation, while statutory damages for intercepting transitory communications are $10,000 per violation.41 One federal court has held that an unopened e-mail constitutes a stored communication for the purposes of the ECPA, and that the intentional and unauthorized access to an unopened e-mail may lead to liability equivalent to $1,000 per violation.42 Employers need to be cognizant that their voice-mail systems may be mail systems today store telephone phone messages electronically on a computer server. Thus, the ECPA would prohibit accessing (listening) of these telephone messages unless the employer's activities falls within the ECPA's exceptions.

In addition to the ECPA, there are other federal statutes which may touch on the issue of electronic monitoring. One such law is the Economic Espionage Act of 1996 (EEA)." The EEA criminalizes theft of trade secrets, even if the secret electronic files are copied onto a diskette owned by an employee." The law closed a loophole in criminal statutes that required there be a theft of physical property. Arguably, when an Ale is copied onto a diskette or other magnetic medium, there is no taking of physical property. Other federal statutes which may be relevant on the issue of electronic monitoring are: the Mail Privacy Statute," the Cable Communications Policy Act," the Privacy Act of 1974," the Fair Credit Reporting Act," the Privacy Protection Act of 1980,48 the Right to Financial Privacy Act,49 the Telephone Consumer Protection Act of 1991,50 and the Federal Records Act.51 Depending on the facts of a particular case, it may be prudent for a concerned employer or employee to research these laws.

The New Jersey Wiretapping and Electronic Surveillance Act (WESA) is New Jersey's analogous statute to the ECPA, and the two statutes are similarly structured.52 The WESA provides for both civil and criminal liability,53 and contains both a "consent" exception54 and the "ordinary course of business" exception. Like the ECPA, the WESA is divided into two provisions that separately address stored communications' and transitory communications.55 Furthermore, punitive damages are available for the interception of transitory communications,56 while only compensatory communications are available for an unauthorized access of stored communications.57

Employer Destruction or Alteration of Stored Employee Communications

While the ECPA and the WESA deal exclusively with a party's privacy interest in their electronic communications or documents, other statutes protect a party's property interest in their electronic communications or documents. For example, New Jersey has two statutes that address the civil and criminal liability of a defendant who has deleted, altered, or committed any other similar destructive act to data belonging to another. It is possible that these two New Jersey statutes might be construed in a manner which creates an employee property interest in electronic communications and documents.

An "unreasonable intrusion" is measured from the standard of what a reasonable person would find "highly offensive," and the tort consists of an intentional intrusion into the "private affairs or concerns" of another.)

August 1999
First, the civil statute does not indicate whether the destroyed data must be on a computer system belonging to a party other than the defendant in order for a claim to be properly maintained.

N.J.S.A. Section 2A:38A-3 (the civil statute) provides that a party who destroys, alters, damages or takes the electronic data of another may be liable for damages to the owner of the data. Because employees often have personal data on an employer’s computer system, a New Jersey employer should think twice before knowingly or purposely deleting these tiles without employee authorization. The civil statute has yet to be interpreted by the courts, and consequently, two important issues remain unclear.

First, the civil statute does not indicate whether the destroyed data must be on a computer system belonging to a party other than the defendant in order for a claim to be properly maintained. This is relevant because the destroyed data (or altered, etc.) was probably stored on the employer’s own computer system. Second, although the civil statute includes intangibles within the scope of its protection, it does not indicate who is deemed to own the intangible data once it is loaded onto the employer’s computer system. Despite these ambiguities, N.J.S.A. Section 2A:38A-3 may be a source of employer liability if the employer takes steps to “cleanse” its computer system of employee data.

Under the civil statute, an employer may be liable for damages equaling: (1) the fair market value of the data provided that a both “willing buyer and willing seller” exist, or (2) the cost of “generating or obtaining [new] data and storing [it] within a computer or computer system.”

In addition to civil liability, such activities may open a New Jersey employer up to criminal liability. N.J.S.A. Section 2C:20-25 (the criminal statute) provides for criminal liability and it utilizes similar language to Section 2A:38A-3. The criminal statute states that a party is guilty of “computer theft” if the party knowingly or purposely damages, alters, destroys or takes the data of another without authorization. The degree of the criminal penalty for committing “computer theft” is dependent on the monetary value of the destroyed data.” Unfortunately, the criminal statute suffers from the same ambiguities as the civil statute.

Suggested Protocol for Employers

Employers would be wise to implement a formal, written policy that governs the use of its computer system and addresses issues of electronic privacy. The policy should also account for other computer and Internet issues that are not the subject of this article. Such as copyright and trademark infringement, defamation, sexual harassment, and document retention policies. Moreover, new computer and online legal developments occur continually. For example, Virginia has recently passed a statute barring public employees from the unauthorized retrieval of sexual material on state-owned computers. This law was found to be constitutional and must be accounted for when drafting a computer and Internet policy for a Virginia employer.

As to the monitoring policy, all employees should manifest their assent to its terms, preferably in writing, and the key points should appear on the log-in screen of every employee’s computer so that the employee’s expectation of privacy will be “refreshed” upon each computer use. The log-in screen should also tell the employee where a copy of the full policy is available, and the computer should condition entry into the system upon acceptance to the terms of the policy.

A strict policy may disallow any personal use of the computer system whatsoever, but a more liberal policy may allow for some personal use and, consequently, a larger expectation of privacy. Either way, however, the policy should clearly state that the computer system and its contents are the property of the employer and that the system is to be used primarily for business purposes. Policies which state that the computer system may only be used for business purposes but that are not enforced, open the employer to attack that enforcement against the plaintiff was selective or discriminatory. If the e-mail system is used by employees seeking a ride home from work, announcing a birthday, selling a car, or for other personal reasons, the employee may claim that the employer should be estopped from selectively enforcing the policy. Moreover, an employee may claim that he or she was singled out due to race, sex, age, religion, national origin, or disability. Employers must exercise common sense in drafting such policies. Just as an employer may not ban use of the company phone system for personal calls, it may not be practical to prohibit employees from using e-mail for any personal messages. Employers must balance the desire to maintain a pleasant work environment with the need to implement sensible computer policies.

An employer’s electronic privacy policy should be drafted in a manner which alerts employees that all employer computers may be monitored at any time. The scope of such monitoring may include: (1) all electronic documents or communications stored in the computer system; (2) all electronic information or communications sent, received or stored with the aid of the employer’s computer system; and (3) all other manifestations of electronic data or information that reside on the computer system regardless of who may own the data or information, and regardless of whether it resides on the computer system for a transitory, temporary or permanent amount of time. Having such a policy will diminish the employee’s expectation of computer and Internet privacy, and it may have the legal effect of constituting employee consent to electronic monitoring.

Regardless of whether an employer would like a strict or a liberal policy, the policy should articulate detailed specifics about the monitoring process.
The policy should effectively communicate who will be doing the monitoring, when the monitoring will be done, how the monitoring will be accomplished, why the monitoring is being conducted, and what types of computer uses are included within the scope of the monitoring process. By precisely defining these details, it is easier for a court to identify whether an employee expectation of privacy was reasonable and whether the employee had in fact consented to electronic monitoring.

Finally, the policy should also explain that an employee does not have an ownership interest in any data or information that resides either permanently or temporarily on the employer’s computer system. The policy should also clearly state that employees may not copy or load software, data or other information onto the employer’s computer system. Employees should be given notice that any information stored on the computer system may be deleted or destroyed at any time and at the discretion of the employer. The inclusion of these provisions in a written policy may help an employer avoid potential liability under N.J.S.A. Section 2A:38A-3 and Section 2C:20-25.

Conclusions on Employee Privacy

There are many issues of employee privacy that may arise in the workplace, and the nature of an employee’s reasonable expectation of electronic privacy in the workplace has become a growing concern of many employers. Just as employees may reasonably expect that they have a privacy interest in their personal mail delivered by the post office, employees may also believe that they possess a similar degree of privacy in their electronic mail. An employee may also believe that their computer files are just as private as the documents they store at the workplace in their personal office, desk or filing cabinet. However, employers have a justifiable interest in the oversight of business-related employee communications, and in the use of its costly computer systems. These two interests must be weighed against each other in ascertaining whether an employer has violated the privacy of an employee. Consequently, an employer may wish to implement a procedure of electronic monitoring so as to ensure that the systems are being used at least primarily for business purposes as opposed to solely business purposes.

At the same time, a well-drafted computer policy can decrease the probability of an employer having to engage in a drawn-out litigation with an employee, and it can help mitigate the potential hardships that result from the uncertainty of judicial precedent in the computer age. These policies can be used to decrease the employee’s workplace expectation of privacy, and they may also serve as a shield if an employer is on the defending side of a lawsuit.

Part II: Student Privacy Interest

The increasing wealth of online information can make the Internet an invaluable and creative source of educational materials for students in the public schools. At the same time, however, the Internet harbors much information that may be properly deemed inappropriate for viewing by children. Students can easily locate such online content as pornography, hate speech or even instructions on how to build dangerous explosives. Furthermore, school children may be easily tempted to share personal information with anonymous and ill-intentioned persons, or to use the school’s e-mail system to send or receive inappropriate communications. Despite these problems however, many school systems will continue to exploit the educational potential of the Internet, while, at the same time, instituting a policy to prevent children from online harms. Such a policy may include supervision of students’ use of Internet filtering software, and the utilization of electronic monitoring.

Electronic monitoring and content filtering are now more important than ever because the courts have been consistently striking down congressional attempts to regulate Internet content objectionable to school children. The U.S. Supreme Court first struck down relevant provisions of the Communications Decency Act, and then, more recently, a district court enjoined the government from enforcing the Child Online Protection Act (COPA).

COPA required online providers of adult content to verify the age of an Internet user before the user may access the objectionable content. COPA was enacted to keep students and other children away from objectionable content. In the event that the injunction is not lifted in a future proceeding, then COPA will not be able to stop adult content from reaching children. In the case of Mainstream Loudoun v. Board Of Trustees OF the Loudoun County Library, the court held that it was unconstitutional to filter out content for adults, however it was permissible to do so for children.

Student Internet use triggers many legal concerns. This segment of the article, however, is limited to addressing the legal implications of electronic monitoring. Furthermore, this article will suggest protocol that a public school system may wish to implement in order to avoid liability for an improper invasion of a student’s “electronic privacy.” The legal issues that this article examines is somewhat interrelated with the issues discussed above in the context of employees.

Constitutionally Permissible Searches

A student’s legally protected privacy interest might be implicated when school personnel search the student’s electronic communications or documents. In substance, by monitoring electronic communications, a public school may be conducting a “search” under the provisions of the
Assuming arguendo, that students have a reasonable expectation of privacy in their electronic communications and documents, the Fourth Amendment will still permit a search if the search is reasonable.\textsuperscript{83}

Fourth Amendment of the U.S. Constitution. Because a public school is a creature of the state, it may only conduct such searches if the search satisfies specific constitutional requirements. In the event that a school conducts a search that is an alleged invasion of privacy, a court will first inquire whether the student had a reasonable expectation of privacy in the subject matter of the search. If the answer is in the negative, then the inquiry ends since there would be no Fourth Amendment invasion of privacy. If the answer is in the affirmative, then the court will look to see if the search was reasonable. If the search was unreasonable, then a court may find an improper invasion of the student’s privacy.

An unresolved issue is whether it matters who owns the computer or media on which an electronic document is stored (or being transmitted). It remains to be seen if a student has a reasonable expectation of privacy in the electronic communications or documents that they store or transmit with the aid of a computer owned by the public school itself. Although no court has addressed this issue directly, an analogy may be attempted in order to predict how a court might rule in the future.

In the case of New Jersey v. Engerud, the New Jersey Supreme Court held that students may have a reasonable expectation of privacy in the contents of their school locker.\textsuperscript{74} This was because students commonly keep their personal effects in their locker, as the school locker becomes their “home away from home.”\textsuperscript{75}

In reference to the fact that the school itself owned the locker, the Court stated that “the Fourth Amendment protects people, not places.”\textsuperscript{75} In addition, students are justified in believing that the administration will only use the “master key” to open the locker at the student’s request.\textsuperscript{75} It should be noted, however, that the Court stated that an expectation of privacy may not have existed if “the school carried out a policy of regularly inspecting students’ lockers.”\textsuperscript{75}

Other jurisdictions have held that there can be no expectation of privacy in a student locker.\textsuperscript{78} One case held that a school had the right to inspect because it had assumed joint control of the lockers.\textsuperscript{79} Another case held that a school has the power to consent to a locker search.\textsuperscript{80} On one occasion, the United States Supreme Court expressly refrained from deciding whether a student is capable of having a reasonable expectation of privacy in a locker, desk or any other “school property provided for the storage of school supplies.”\textsuperscript{81}

If the “locker cases” are applied to a situation entailing student use of school-owned computers, it is unclear whether a court would find a reasonable expectation of privacy. Certainly, if students or their parents are not on notice regarding a policy of electronic monitoring, the chances are greater that a court may find a reasonable expectation of privacy. Furthermore, the reasonableness of an expectation of privacy may depend on whether the school has a policy of allowing or disallowing students to store documents or e-mails on the computer system itself or on a floppy disk owned by the student. At the very least, a school district’s “search” is more likely to withstand constitutional scrutiny if it has provided notice to all students and parents that use of the computer system by students is subject to electronic monitoring at any time. The probability of such a finding may be increased if the school has the written assent of students and their parents to the school’s computer policy.

Assuming arguendo, that students have a reasonable expectation of privacy in their electronic communications and documents, the Fourth Amendment will still permit a search if the search is reasonable.\textsuperscript{84} The requirements of “probable cause” do not have to be satisfied.\textsuperscript{85} Rather, the standard of reasonableness is intended to reflect a balance between a student’s privacy interest and the school’s interest in maintaining student discipline.\textsuperscript{84}

In New Jersey v. T.L.O., the United States Supreme Court held that a student search is reasonable, hence permissible, when there are “reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school.”\textsuperscript{86} This governs the requirement that a search must be “justified at its inception,” however a search must also be reasonable in its scope.

To be reasonable in scope, the search must be “reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.”\textsuperscript{87} For example, if a student reports that he or she has been sexually harassed by an e-mail sent by another student, it might be reasonable for a school official to search all of the electronic communications between the two students. At the same time, however, it might be unreasonable for the school to search any electronic communications between the harassing student and his or her family or of other students not implicated.

In both Engerud and T.L.O., the school’s search was based on a suspicion that a particular person may have been breaking the law or the rules of the school. The courts refer to this concept as individualized suspicion. However, in the context of electronic monitoring, a school might not only be monitoring particular students based on an individualized suspicion; the school may choose to monitor all students’ electronic communications and documents. The United States Supreme Court has expressly refrained from deciding whether individualized suspicion is demanded by the Fourth Amendment in order for an otherwise reasonable student search to remain so.\textsuperscript{88} Generally, however, exceptions to the rule of individualized suspicion have been recognized where the privacy interests implicated are minimal and there are other safeguards “to assure that the individual’s reasonable expectation of privacy is not subject to the discretion of the official in the field.”\textsuperscript{89}

In the case of Desilets v. Clearview Regional Board of Education, the New Jersey Supreme Court held that
Jersey Appellate Division held that a school official could search student hand luggage without individualized suspicion when the search was conducted in conjunction with a field trip and the search was for contraband. The Desilets court emphasized that the school's policy was upheld because school officials did not retain the discretion to decide who should be searched. Furthermore, schoolchildren had advance notice of the search and, as such, they could have either refrained from bringing hand luggage on the trip altogether or they could have removed highly personal items from their hand luggage prior to the field trip. Interestingly, the Desilets court did not emphasize in its holding the fact that the schoolchildren's parents had expressly consented to the contraband search.

The holding of the Desilets court might be applicable in the context of electronic monitoring in the public schools. A school board may wish to institute an electronic monitoring policy in which the electronic communications and stored documents of students may be indiscriminately searched by some previously announced method. Such a policy should provide for the monitoring of all students or it should contain a prescribed "formula," devised in advance, to monitor a randomly and indiscriminately chosen student. The policy should also state the school interests in monitoring the electronic communications and documents of students.

Such interests may include, but are not limited to: (1) preventing the downloading of inappropriate materials from the Internet (e.g., pornography); (2) preventing the use of the e-mail system to harass or defame another; (3) preventing the unauthorized downloading of materials protected by copyright; (4) preventing the use of the computer in a manner inconsistent with school rules that properly foster discipline; (5) preventing the use of the school computer system for general, non-educational purposes; (6) preventing students from revealing personal information over the Internet (via e-mail or the World Wide Web); and (7) preventing students from perpetrating computer crime.

A Fourth Amendment claim for invasion of privacy may usually be found in the context of either a Section 1983 action or in a motion to suppress evidence in a criminal proceeding. First, Section 1983 provides a cause of action for damages against state actors when they violate an individual's federal constitutional rights under color of law. Furthermore, a state actor may be subject to qualified immunity from suit depending on the law of a particular state. Second, the exclusionary rule provides for the suppression of evidence discovered during an improper student search. The exclusionary rule is not universally accepted by all jurisdictions, however it is followed in New Jersey.

Common Law Tort Actions

Many jurisdictions allow a tort action if there has been an unreasonable intrusion upon the seclusion of another. Similar to the constitutional action, the tort action protects an individual's privacy interest. However, unlike a constitutional action, a tort action may be barred by a state's Tort Claims Act if the action is against a state actor. As such, the availability of a tort remedy for an invasion of privacy may be severely impaired when the action is brought against a school district. Consequently, an aggrieved student may be more "successful" in bringing the claim as a constitutional action.

Federal and State Statutory Actions

A school monitoring policy may also implicate the provisions of the ECPA when school officials intercept transitory student communications or when they gain unauthorized access to stored student communications. The issue of "consent" has special relevance to the ECPA's application to a public school setting. As discussed in Part I, any claim of an ECPA violation can be defeated by a showing that the plaintiff had consented to the defendant's activities. It is unclear, however, whether the student must consent to the school's monitoring policy, whether the student's parent or guardian may consent on behalf of the child, or whether the school itself can satisfy the consent requirement under the doctrine of in loco parentis.

In the case of Pollack v. Pollack, the Court of Appeals for the Sixth Circuit held that under the ECPA, the "consent" requirement may be satisfied under certain circumstances if a parent consents and the parent can demonstrate a "good faith, objectively reasonable basis for believing such consent was necessary for the welfare of the child." In Pollack, a mother had recorded a telephone conversation between her child and the child's father without authorization. The mother and the father were ex-spouses. The court held that the mother did not violate the ECPA since one party need only consent to the recording, and because the mother's consent would suffice as consent on behalf of the child. At the time of the recording, the mother had custody and was the child's legal guardian.

In rendering its opinion, the Sixth Circuit relied on similar conclusions reached by the Second, Seventh, and Tenth Circuit Courts of Appeals. The Sixth Circuit also relied on a similar conclusion reached by a New Jersey court interpreting the WESA. While the Sixth Circuit's holding was based on a theory of "vicarious consent," the court noted that other jurisdictions had reached similar conclusions by holding that the ECPA "business use exception" was satisfied when a parent taped telephone conversations within the home. This is because such interceptions and tapings have been considered to fall within the scope of the exception's language that allows interceptions that are, "within the regular course of business."

Although the holding of Pollack does not directly address electronic monitoring in the schools, it may be applied by analogy. First, there appears to be a basis to argue that a parent may consent in place of the child provided that the parent satisfies the good-faith requirements of Pollack. Second, if the parent could have consented in place of the child, there may also be an argument that the school itself may satisfy the consent requirement due to

The issue of "consent" has special relevance to the ECPA's application to a public school setting.

August 1999
the doctrine of in loco parentis. Third, a school may attempt to argue that its allegedly offensive electronic activities are "within the regular course of its business"; i.e., that the school is monitoring in order to prevent the child from incurring or causing harm to himself, other students, or the school’s computer system.

Related Policy Concerns

In drafting a computer and Internet policy, a school board should account for all relevant legal issues, such as: (1) electronic privacy; (2) sexual harassment; (3) objectionable Internet content and the use of filtering software (i.e., pornography); (4) copyright infringement and plagiarism; (5) trademark infringement; (6) the intentional or accidental destruction or alteration of student data; (7) computer crimes (i.e., hacking); (8) student freedom of expression on the Internet and in e-mails; (9) online defamation; (10) the availability of personal student information over the Internet; (11) the use of the computer or the Internet to sell drugs or commit other non-electronic crimes; and (12) the use of the computer or the Internet to break school rules.

For example, a school policy should account for issues of "electronic" sexual harassment. This is because school e-mail systems provide students with an opportunity to sexually harass other students for which school districts may be held liable. Recently, the U.S. Supreme Court held that school boards may be liable for acts of sexual harassment committed by a student against a classmate if the school board has acted with "deliberate indifference" and has "exercise[d] substantial control over both the harasser and the context in which the known harassment occur[ed].""100 Presumably, this new rule of law would apply to acts of sexual harassment committed with the aid of the school's e-mail system. A school district may attempt to avoid liability by implementing a policy that forbids the use of the computer system for harassment purposes and which prescribes in advance the appropriate disciplinary measures for those who electronically harass other students. Schools should also implement an appropriate discipline upon discovering that one student is sexually harassing a classmate.

The computer and Internet policy should also provide notice of the basic rules and procedures for use of the computer and Internet by students. The policy may provide that the computer system be used primarily for educational or career related purposes. A school board should include additional guidelines if student organizations will be permitted to create and maintain their own web site. School web sites create additional student privacy issues. School districts must decide whether the web site will be available to anyone or whether web site access will be limited by password to students, faculty and parents. School boards must also take care not to publish sensitive and personal student identification information on school web sites such as last names, addresses, phone numbers, student photographs, etc. Finally, it would be prudent for a faculty member to act as a "gate-keeper" for all content to be posted on the school's web site. This person can make sure that the privacy and other related policies are being followed (i.e., concerning, discrimination, copyright infringement, defamation, etc.).

Conclusion on Student Privacy

School computers and school access to the Internet may function as a useful educational tool, as they are effective sources of endless information and communications capabilities. Unfortunately, however, the advantages of computers and the Internet are not available risk-free. There are many dangers to be aware of when a child uses a computer, the Internet, or even an in-house e-mail system. It is well established that schools have a duty to supervise children so that students do not cause harm to themselves, others, or property. For this reason, and in today’s political climate, a school board may choose to implement protocol which provide for the monitoring of electronic communications and documents.

In implementing such a policy, it is best advised for a school board to fully disclose to students and parents the full nature of the monitoring and for it to expressly state the complete scope of the monitoring process. After doing so, the school should acquire the consent of both the student and the student’s legal guardian(s) so that the school may intercept transitory communications and access stored electronic documents without opening itself up to an unnecessary risk of liability under the ECPO or the WESA. Furthermore, a student’s expectation of privacy in the school computer system may be diminished by notifying students that the computer system may be used primarily for educational purposes and that the school reserves the right to monitor or access all computer data at any time. By implementing a firm policy and by providing notice to all involved parties, a school board may conduct electronic monitoring with the greatest amount of certainty that the school board will be complying with applicable law.

Endnotes


2. See Figured, 231 N.J. Super. at 256.


4. Id.


8. See Figured, 231 N.J. Super. at 256.


14. Id. at 716.

15. Id.

16. Id. at 717.

17. See id.

18. See Ortega, 480 U.S. 718.

19. Id.

20. Id. at 719.

21. Id. at 723.

22. See id. at 726.

23. See id.


25. See id.

26. Id. at 98-99.

27. See ONLINE LAW: THE SPA’S GUIDE TO DOING BUSINESS ON THE INTERNET, 412-13 (Thomas J. Smedlinghoff, ed. 1996)
New York Law

Sources of NY Law
www.nyu.edu/law/library/nycl.html
Identifies books for purchase that include the New York City Charter and Administrative Code
www.nypl.com/links/civindex.html provides a guide to the operations of Civil Branch of Manhattan’s Supreme Court.

Environmental
www.epa.gov

Statutes
Cornell www.law.cornell.edu/topics/state_statutes.html

State Courts
www.mssc.state.ms.us
www.appellate.courts.state.ak.us
www.state.nj.us/judiciary

Endnotes
1. An “internet” is a network that is a collection of networks interconnected with routers. The internet is the largest network in the world. Webber, *Using the Internet for Legal Research* (ALI-ABA 1998) (see Appendix B).
2. Note that URLs generally have “http://” in front of “www.” Others may have separate notations. In most cases, typing “www.” before the rest of the URL should be sufficient. In any event, I have not included the “http://” before each URL listed here.
3. Use of “+” and “-” are limiting features. The + looks for the specific word, and not synonymous words, and the - will not include search results with those words.

Steven Richman is a partner at Gallagher, Brody & Butler, practicing commercial and international law in Princeton. He is chair of the New Jersey Lawyer, the Magazine Editorial Board and president of the Plainsboro Public Library Board of Trustees.

Employee and Student Privacy

continued from page 30

30. 18 U.S.C. §§ 2511(1).
32. Supranote 27, at 414 (citing *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983)).
33. Supranote 27, at 414 (citing *Epps v. St. Mary’s Hosp. of Athens, Inc.*, 802 F.2d 412 (11th Cir. 1986)).
34. See supra note 27, at 414 (citing *Brogg v. Am. Air Filter Co.*, 630 F.2d 412 (5th Cir. 1980)).
37. See *e.g.* *Williams v. Poulos*, 11 F.3d 271 (1st Cir. 1993).
38. See *e.g.* *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992).
42. See id at 463.
52. 44 U.S.C. §§ 2101 et seq., 2501 et seq., 2701 et seq., 3091 et seq., 3101 et seq., 3301 et seq. (1999).
55. **N.J.S.A. § 2A:156A-3; see also N.J.S.A. § 2A:156A-27.**
56. **N.J.S.A. § 2A:156A-4(d).**
57. **N.J.S.A. § 2A:156A-2(d)(1).**
59. **N.J.S.A. § 2A:156A-3.**
62. § 2A:38A-1 et seq.
64. § 2C:20-23 *seq.* (1999).
65. **N.J.S.A. § 2C:20-25(a).**
66. **N.J.S.A. § 2C:20-26.**
67. CodeR.5
68. *Supp. Michie*
70. v. *Reno, 521*

72. See id. at 337 n.5.
73. See T.L.O., 469 U.S. at 341.
74. See id. at 339.
75. See id. at 342.
76. See id. at 341.
77. See id. at 342.
78. T.L.O., 469 U.S. at 342 n.9.
81. See id. at 381-82.
82. See id.
83. See id. at 372 (stating that the student’s mother had read then signed a “permission slip” consenting to the search).
84. T.L.O., 469 U.S. at 333 n.3.
87. *See id.* at 610 (citing *Janeckav v. Franklin*, 843 F.2d 110 (2nd Cir. 1988)); Anonymous v. Anonymous, 558 F.2d 677 (2nd Cir. 1977); *Scheib v. Grant*, 22 F.3d 149 (7th Cir. 1994); *Newcomby v. Ingle*, 944 F.2d 1534 (10th Cir. 1991)).
88. See id. at 608-09 (citing *State v. Diaz*, 308 N.J. Super. 504 (App. Div. 1998)).
89. Davis v. Monroe County School Board of Education, 1999 U.S. LEXIS 345228.
90. See id.

Richard L. Ravin is a member of the law firm Ravin, Sarasohn, Cook, Baumgarten, Fisch & Rosen, P.C. in Roseland and is head of the firm’s Internet, Computer and Intellectual Property Law Department. He is also the co-chair of the Internet Law Committee for the Intellectual Property Law Section of the New York State Bar Association. Steven E. Halpern is a third-year law student concentrating in Intellectual Property at Seton Hall University School of Law. He is also a summer associate with the firm. Copyright 1999, Ravin, Sarasohn, Cook, Baumgarten, Fisch & Rosen, P.C. All Rights Reserved.