The word “Cyberspace” has become the household word of the 1990’s, though most people have no idea what Cyberspace is or how it works. Many know that it is the information highway where ATM machines, telephone calls, fax transmissions, and computers somehow magically travel.

In reality, Cyberspace consists of electron states, microwaves, magnetic fields and light pulses. As such, it is the repository for all digital and electronically transferred information.¹ Cyberspace encompasses all electronic messaging and information systems including: Bulletin Board Systems (“BBS”);² commercial data services; research data networks; electronic publishing; public and “private”³ networks and network nodes; e-mail⁴ systems; data banks with personal medical, credit, membership, purchasing habit, and census information; electronic data interchange systems; and electronic fund transfer systems.⁵

The Internet,⁶ a mere portion of Cyberspace, is an immense network of networks that connects an estimated twenty million computer users by telephone lines to thousands of electronic information storeshouses worldwide.⁷ With increased accessibility to the Internet, privacy is a major issue.⁸ A single computer is now the equivalent of a typewriter, teletype, filing cabinet, printing press and more, all wrapped into a few small pieces of equipment that are now sitting in millions of homes and offices. In effect, a new mass media is emerging before our eyes.

The purpose behind the Internet is increased accessibility and shared communications. People from all over the world can communicate and share information with little more than a few keystrokes.⁹ However, with the increased accessibility and increased number of users comes prodigious and predictable opportunities for the invasion of one’s privacy.¹⁰ Additionally, the essence of shared

² A BBS is an electronic network of computers. At the heart of the BBS is the central computer, set up and operated by the system operator. Users link their computers to the central BBS computer by modem, which is a device that allows computers to communicate over telephone lines. Once users have accessed the BBS, they may communicate with other users, obtain information from databases, obtain software, or perform other activities “on-line.” Eric Schlacter, Cyberspace, The Free Market and the Free Marketplace of Ideas; Recognizing Legal Differences in Computer Bulletin Board Functions, 16 HASTINGS COMM. & ENT L.J 87, 90 (1993).
³ E-mail is electronic mail sent via computer.
⁵ Many have tried to come up with the perfect, most understandable definition of the Internet. It is the world’s largest network of computers. A network is the term for a group of computers linked together so they can share information and resources. The Internet is not a single network, but a network of networks. The Internet grew out of a United States Defense Department experiment in the late 1960’s for linking military networks. The experiment grew into connecting the networks at other research institutions and universities, and more recently to connect commercial users as well. MARK GIBBS, NAVIGATING THE INTERNET, 2-5 (1993).
⁸ In the Gulf War, CNN provided unprecedented news coverage that was nearly instantaneous by television news standards. However, the Internet, which at that time linked 15 million people directly and as many as 25 million through private networks, provided a completely unmediated channel of communication that allowed news of Gulf events to travel swiftly to many people. As one Internet user wrote: “In the Gulf War news coverage, we were the watchers, dependent on a few men and women with cameras and a company with the technology to bring those images home to us. On the Internet, we are the reporters, the viewers, and the production team.” Clemons P. Work, Whose Privacy?, 55 MONT. L. REV. 209, 209 n. 111 (1994) (citing TRACY LAQUEY & JEANNE C. RYDER, THE INTERNET COMPANION, 2-3 (1993)).
⁹ For example, in 1991, Dutch computer “hackers” had no trouble breaking into the U.S. government’s Pacific Fleet Command and Kennedy Space Center Computers. In addition, direc—
communications gives rise to questions of ownership and expectations of privacy.\(^9\)

The rapid growth of computer technology has left the law in the dust. There are limited laws regulating Cyberspace, and many of its users and program activities remain unchecked. Abuses have occurred, and if the history of the development of other forms of communication is any guide, more far-reaching abuses affecting many more people will occur. The very anonymous nature of the Internet (and all Cyberspace) has as much potential for private and governmental abuse as a masked burglar, a con artist, a hooded night rider, or a dossier collecting zealot. The paradox is that in order to protect privacy, anonymity must be limited.

This Comment explores the evolution of the privacy issue in Cyberspace and, more specifically, the Internet. Part I defines the Internet and its recent technological advances. Part II explores the Constitutional and common law history involving computer communications. Part III delineates the deficiencies in the current law and the currently proposed answers to the privacy dilemma. Part IV offers a possible solution, recommending a plan for Federal Communications Commission ("Commission" or "FCC") and Congressional action. Though this Comment will focus only upon the legal issues involving privacy in Cyberspace and the Internet, there are many other pressing legal questions that will require answers in the coming years.\(^11\)

.I. THE EVOLUTION OF PRIVACY LAW

A. Constitutional History

Several constitutional amendments directly and indirectly address privacy issues, including: the First Amendment, prohibiting laws abridging the freedom of speech, assembly, or the press; the Fourth Amendment, protecting people and property from unreasonable government intrusion; and the Fifth and Fourteenth Amendments, guaranteeing due process of law and exemption from self-incrimination. The Fourth Amendment of the United States Constitution has particular implications to the issue of privacy on networks such as the Internet. The Fourth Amendment states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.\(^12\)

Cyberspace has no physical boundaries, and a "seizure" in Cyberspace may not result in a loss of property or liberty as the Framers of the Constitution contemplated. Under the Fourth Amendment, an individual's "papers" are safe from "search and seizure," but it is unclear whether the protection of paper applies when the papers are electronic bits of information and lack physical presence.

Cyberspace civil libertarians would alter Potter Stewart's famous words to read: "The Fourth Amendment and the personal rights it secures have a long history. At the very core stands the right of a man [and woman] to retreat into [his or her] home [turn on the computer, log into Cyberspace] and there be free from unreasonable governmental intrusion."\(^13\)

Some argue that Cyberspace must be subject to the same or stricter laws that apply to public mails, telephones, and broadcast airways in order to protect all users of the Internet and similar technology.\(^14\)

Katz v. United States\(^15\) is one of the most pivotal cases regarding the Constitutional right to privacy and electronic communications. Katz involved a "bug" or listening device that the government placed on the outside of a public telephone booth.\(^16\) The

---

\(^9\) Such issues include: whether owners of copyrighted material can protect their rights when their works may be accessed and downloaded by thousands or millions of computer users; and whether computer users have the right to communicate with each other freely without having their statements censored by owners of the computer gateway providers. Mike Godwin, The

\(^10\) The rapid growth of computer technology has left the law in the dust. There are limited laws regulating Cyberspace, and many of its users and program activities remain unchecked. Abuses have occurred, and if the history of the development of other forms of communication is any guide, more far-reaching abuses affecting many more people will occur. The very anonymous nature of the Internet (and all Cyberspace) has as much potential for private and governmental abuse as a masked burglar, a con artist, a hooded night rider, or a dossier collecting zealot. The paradox is that in order to protect privacy, anonymity must be limited.

---


\(^12\) U.S. CONST. amend. IV.

\(^13\) Potter Stewart's original words were: "The Fourth Amendment and the personal rights it secures have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." The Quotable Lawyer 253 (David Shrager & Elizabeth Frost eds., 1986).


\(^15\) 389 U.S. 347 (1967).

\(^16\) Id. at 348.
government argued that because the bug was not actually inside the booth, there was no invasion of privacy. The defendant argued that the placement of the bug violated the Fourth Amendment's search and seizure clause. The Supreme Court held that "the Fourth Amendment protects people, not places." What a person knowingly exposes to the public, even in her own home or office, will not receive Fourth Amendment protection. But what she seeks to maintain as private, even in an area accessible to the public, may be constitutionally protected.

The issue then becomes whether a person sending an e-mail message on the Internet has a reasonable expectation of privacy when twenty million people use the same service. In addition, a more difficult privacy question concerns whether the government can access a person's or an organization's database to learn what kind of databases are used, what searches were run and what type of information has been retrieved.

The Constitution protects citizens from unlawful intrusions into their privacy by the government, but does not protect citizens from privacy invasions committed by private citizens. Legal causes of action provide protection against invasions of privacy by private citizens, such as the torts of invasion of privacy and trespassing. However, applying old laws to ever-advancing technology may not be sufficient.

B. Statutory History

Radio and television communications are subject to regulation by the FCC and by the Congress. However, the FCC considers computer information systems to be "enhanced services" beyond the scope of its regulatory power.

Congress has enacted several laws that address privacy issues. However, with the advent of new technology, such as the Internet, current laws are becoming more and more obsolete. These laws include: The Federal Wiretap Act of 1968; the Privacy Protection Act of 1980; the Electronic Communications Privacy Act of 1986; and finally, the Computer Fraud and Abuse Act of 1986.

In addition to federal law, many state laws apply to computer communications. However, problems arise with jurisdictional issues, as the very nature of the technology is multijurisdictional.

1. The Federal Wiretap Act

Congress created The Federal Wiretap Act of 1968 ("Wiretap Act") to address the privacy issues in wireline communications between two persons. However, the law only affected "wire communication," which is limited to "aural [voice] acquisition." In United States v. Seidlitz, the court held that the interception of computer transmission is not an "aural acquisition" and, therefore, the Wiretap Act does not cover transmission or stored computer data.

2. Privacy Protection Act

The Privacy Protection Act of 1980 ("Privacy Act") protects electronic bulletin boards and publicly accessible computer networks. The Privacy Act operates to prohibit blanket searches and seizures of such entities unless there exists "probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate . . ." and such criminal offense does not consist of the "receipt, possession, communication, or withholding of such materials . . ."

Cyberspace legal scholars interpret the practical effect of the Privacy Act to:

held that a newspaper office could be searched even when no one employed by the paper was suspected of any crime. Most on-line service providers operate on an interstate basis. Even a few, infrequent, out-of-state calls can warrant interstate status. Rose, supra note 4, at 4.

See Hernandez, supra note 20, at 1.


Id.


In particular, Harvey Silverglate, Thomas Viles, Mike
strictly limit wholesale computer seizures where the systems are used for bulletin boards or other general communications. In such situations, a seizure is appropriate only where the system's operators are directly implicated in unlawful activity. [However,] where the system has been used as a conduit by others who are criminally motivated, but the operator is not involved, the Privacy Protection Act would seem to require that no search take place, but instead a subpoena be issued for the relevant information.44

The Attorney General has issued guidelines under the Privacy Act governing the execution of search warrants where highly confidential or personal information relating to innocent third parties may come into the hands of law enforcement authorities.55 According to the guidelines, federal officials should “not use search and seizure to obtain documentary materials in the possession of disinterested third parties unless reliance on alternative means would substantially jeopardize their availability . . . or usefulness,” or where less obtrusive means of obtaining such materials are available.56 The guidelines define “documentary materials” to include “materials upon which information is electronically or magnetically recorded.”57 Additionally, recognizing the potential for violations of privacy rights of individual third parties, the Attorney General's guidelines exact strict controls over search warrants executed upon records possessed by physicians, lawyers and clergy.58

The first case to apply the Privacy Act to electronic publishers was Steve Jackson Games, Inc. v. United States Secret Service.59 In Steve Jackson Games, the Secret Service investigated Craig Neidorf, a student and publisher of an electronic magazine called "Phrack," for reprinting a document stolen from a Bell South computer.60 The Bell South file was available to BBSs around the country, including one operated by an employee of Steve Jackson Games, a creator and publisher of computer games in Austin, Texas. While looking for evidence against the employee, Secret Service agents searched the bulletin board run by Jackson and found the draft of a rule book for a fantasy game called GURPS Cyberpunk. The government concluded that the manual was essentially a handbook for computer crime.61

The Secret Service then raided Steve Jackson Games, Inc. and seized its bulletin board system, drafts of the game, electronic mail, and all electronic files. They also took all copies of the company's soon to be released game, GURPS Cyberpunk. Jackson was never charged with a crime, and his files and equipment were returned to him four months after the raid.

However, the raid caused the company to shut down and lay off approximately half of its employees. The Electronic Frontier Foundation,62 which provided legal counsel for Steve Jackson,63 analogized the Secret Service's taking to an indiscriminate seizure of all of a business's filing cabinets and printing presses.64

3. Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 198664 (“1986 Act”) closed the gaps left open by the Wiretap Act. Congress originally enacted the 1986 Act in response to Watergate.65 The 1986 Act is the privacy shield protecting e-mail.

The statute provides in part that “any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor
to trial and he incurred approximately $100,000 in legal costs. Id.

43 Id. In May, 1991, Jackson filed suit against the Secret Service, two individual Secret Service agents, an assistant U.S. attorney and others, alleging violations of his Constitutional rights.
44 LEGAL CASE SUMMARY, ELECTRONIC FRONTIER FOUNDATION, May 10, 1990 (on file with the CommLaw Conspectus).
46 Rose, supra note 4, at 1.
to intercept, any wire, oral, or electronic communication" shall be fined or imprisoned. The intentional disclosure or use of the contents of any wire, oral, or electronic communication that is known or could reasonably be known to have been intercepted in violation of the statute is prohibited. In essence, this law prohibits anyone but the sender or the intended recipient from reading an intercepted e-mail message. Any further disclosure or use of the content of the message by any party, other than the message sender and its intended recipient, is prohibited if the intercepting party knows or has reason to know that the message was illegally intercepted.

The 1986 Act enables electronic communication service providers to ensure the privacy of their subscribers and e-mail users. Invasion of privacy problems have arisen repeatedly. The culprits are now dubbed "hackers." A hacker is a computer pirate who violates computer privacy by intercepting and possibly using telephone and credit card numbers, reading electronic mail, listening in on cellular phone conversations, or by tapping into sensitive government databases.

In Steve Jackson Games, the court looked at section 2701 and the following sections of the 1986 Act regarding access to stored computer communications. Section 2701 reads, in part, "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system" shall be subject to fines and/or imprisonment, or both.

Applying the 1986 Act, the court held that the government had to follow the procedures established by section 2703 in order to properly discover the contents of the electronic mail on the BBS. The court went on to say that the Secret Service's evidence of good faith reliance on what it believed to be a valid search warrant was insufficient. The government knew that the computer stored private electronic communications, and therefore the only legal means to gain access to those communications was by compliance with the Act, and not by seizing the BBS.

While the 1986 Act presently is the most comprehensive statute applicable to computer communications, there are many ambiguous provisions. The judge in Steve Jackson Games agreed with the Secret Service that e-mail on Jackson's system was not intercepted when the computers were seized because it was not taken during the transmission. However, the Electronic Frontier Foundation argued that until the intended recipient takes control of the message by reading it, the e-mail should be considered vulnerable to interception.

In October of 1994, the Fifth Circuit affirmed the district court's ruling in Steve Jackson Games. The Fifth Circuit held that because the seizure of the e-mail contents was not contemporaneous with the transmission of the e-mail, there was no "interception" within the meaning of the 1986 Act.

4. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act of 1986 ("Fraud Act") criminalizes unauthorized access to federal interest computers. The Fraud Act defines "federal interest computer" as a computer:

---

47 18 U.S.C. § 2511(1)(a) and (4).
48 Id. § 2511(1)(c).
49 The Presidential Records Act constitutes a possible exception to the privacy of e-mail. The Presidential Records Act requires all records classified by the Act as "Presidential Records" to be preserved for historical research. 44 U.S.C. §§ 2201(2), 2204 (1988). The only case to apply this statute to presidential e-mail held that the Presidential Records Act implied preclusion of judicial review of the President's compliance with its provisions. Armstrong v. Bush, 924 F.2d 282, 290-91 (D.C. Cir. 1991).
51 Intercepted e-mail messages can cause problems for the senders and the receivers. For example, e-mailing off-color jokes to co-workers could get the sender fired; a competitor intercepting a business proposal could reek havoc with the company; and passwords, private phone numbers and credit card numbers easily could be lifted off of private e-mail messages.
52 Also referred to as "phreakers" and "crackers."
(A) exclusively for the use of a financial institution or the United States Government and the conduct consisting the offense affects the use of the financial institution’s operation or the government’s operation of such computer; or (B) which is one of two or more computers used in committing the offense, not all of which are located in the same State.83

One of the most significant cases in the area of federal-interest computer technology abuse is United States v. Robert Tappen Morris.84 On January 2, 1990, Morris, a suspended graduate student at Cornell University, became the first person convicted of a felony under the Fraud Act.85 Morris admitted releasing a worm, similar to a virus, onto the Internet.86 The worm affected network subscribers including the University of California at Berkeley, NASA and the U.S. Logistics Command at Wright-Patterson Air Force Base.87 The estimated cost of the computer down-time and the labor necessary to combat and cure the worm fell between $5 million and $12 million.88

Morris, the son of a top computer security employee at the National Security Agency, denied any intentions to do harm to Internet subscriber’s equipment.89 Regardless of intent, the damage was done. This case demonstrates the need for securing against injury to innocent third parties before the injury occurs.

II. CLIPPER: A POSSIBLE SOLUTION

Imagine that your bank account holds one hundred thousand dollars accumulated only after years of diligent saving. At the time you are ready to withdraw the funds for a home down payment, the teller declares that you must be mistaken. ‘Have you forgotten that you transferred those funds weeks ago?’ she inquires. Upon further investigation the bank finds that someone has accessed your computer system and, using your personal identification number, has transferred and withdrawn your entire balance from a bank in another state or country.

The reality of such a scenario is not impossible. It takes computer gurus only minutes to break into the world’s largest banking computers or a personal computer and take a ride into Cyberspace’s private lives.

As demonstrated by Morris, mass amounts of information can be irreparably harmed and some of the worlds most important computer systems can be infiltrated and destroyed within minutes. While laws may punish the culprits, the damage has often already been done.

The United States government, particularly the Federal Bureau of Investigation and the National Security Agency, has proposed what they consider to be the ultimate prescription for preventive medicine, the Clipper Chip. Clipper, as it often is called, is “the U.S. government-designed encryption system for encoding and decoding phone calls and E-mail so that the communication is protected from snooping . . . .”90 Clipper allows the government to retain a “back door key.” Officials insist this is necessary to be able to intercept messages from mobsters, terrorists, and drug dealers.91

However, many computer and policy experts oppose Clipper, arguing that communications security is too important to be left to “secret processes and classified algorithms.”92 A recent survey interviewing 1,000 Americans reported that two-thirds believed it was more important to protect the privacy of home telephone calls than to preserve the ability of the police to conduct wiretaps.93 When Clipper was explained to the interviewees, eighty percent opposed the idea.94 Yet, the National Security Agency argues that “non-escrowed” encryption technology threatens law enforcement and national security.95

While there are other security and encryption programs, they too have problems and insufficiencies. Most importantly, the programs have been written, encoded, and marketed by private persons. Therein lies the problem. If a private person or group wrote provided for prison time. Morris, 928 F.2d at 504.

83 Id. § 1030(e)(2).
86 While a worm is not usually intended to cause damage, as with viruses, its main purpose is to replicate itself as many times as possible. GIBBS, supra note 5, at 295.
88 Id.
89 Morris was fined and given probation though the statute
the encryption, chances are that a private person or group can break the code. Because the Clipper Chip was written and designed with the benefit of the extensive resources of the Federal Bureau of Investigations and the National Security Agency, it is the system most unbreakable both here and abroad.

The battle over the Clipper Chip will undoubtedly be a long one. It could be years before such proactive security and privacy protections, government implemented or otherwise, would be put in place.

III. THE FCC'S ROLE IN PROTECTING PRIVACY

The FCC has determined that it will not regulate computer communications in any manner different from voice communications. Federal courts have affirmed this decision. Without direction from Congress, the FCC will continue to regard computer communications as being outside their realm of regulation. As privacy issues become more of a concern, pressure will be applied to legislative bodies to pass more comprehensive legislation in an attempt to fill the holes of the currently inadequate laws.

Clearly, according to its stated purpose, the FCC is the most logical body to enforce computer laws. Telephones run the modems that connect and network computers, while satellites transfer data where telephone lines cannot. Thus far, the FCC has regulated the telephone wires that connect telephone and the satellites that transmit audio, video, and data.

With the advent of the new computer technology, the FCC cannot just dig in its heels. The FCC must rethink its position on computer communications as being “enhanced services” outside of the realm of its regulatory power. The FCC has been the governing body of wire and satellite communications up until the computer boom era; it must adjust with advancing technology, just as it did when television technology was created and largely replaced radio.

While current FCC regulations cannot be blankety applied to Cyberspace, and overseeing the governing of this whole new world would be a tremendous undertaking, the FCC is the most logical body for the task. Computers are not some abstract unknown, they are simply the newest means of communications and, as such, mandate regulation.

Civil libertarians do not want computer users' rights trampled upon by government intrusion and regulation. While these concerns are legitimate, it must be remembered that invasion of privacy by hackers and criminals tramples on peoples’ rights with a larger, and arguably a more dangerous foot than the government has ever had. The key to computer privacy regulation must be reasonableness.

But to merely suppose that abuses will not occur flies in the face of human experience. Computers are quickly taking over traditional communication devices. Computers have become the heart of the American person's home, business, military, government, financial, and educational institutions. However, with the ease and convenience of new technology comes new avenues for user exposure to personal, political and business sabotage, and economic loss. A falsely incriminating memorandum placed on a politician's campaign committee hard drive, financial records of a bank manipulated, or draft documents deleted from files at a law office are anonymous invasions of privacy that subject the computer user to relatively untraceable victimization.

The anonymity of the wrong-doer is more secure in Cyberspace. While other forms of communication such as mail, telephone, and facsimile could intrude on the privacy of a person or organization, they could not so easily elicit information or initiate actions without the knowledge of that person or organization. Where is the electronic notary public on the Internet? Anonymity sends a big invitation for abuse.

An expert's mastery of the computer technology gives impending power over those who are novices at the computer. The “experts” have the ability to do harm should they chose, effectively putting the majority of users on the Internet open to great invasions of privacy. The ability to become a victim occurs upon signing on to the Internet and similar networks. It is up to the legislatures to protect the majority from the abuse of the minority whose greater mastery of the technology puts them in a position to victimize the less knowledgeable, hence vulnerable users.

In theory, if there were no laws regulating speed on interstates, cars would travel at excessive speeds

---

76 The Telecommunications Deregulation Sourcebook 259 (Stuart N. Brotman, ed. 1992).

77 See Computer and Communications Industry Association, etc. v. Federal Communications Commission, 693 F.2d 198 (D.C. Cir. 1982) (holding that customer premises equipment and enhanced services are not appropriate subjects for Title II regulation).

78 The nation’s telephone system is heavily regulated by the FCC with standard fees and rules for the exchange of messages between carriers. The broadcast system is regulated as well, with licensing procedures, rules and costs.
thereby putting those who chose to drive carefully in harm’s way. Speed limits impose a balance between the rights of the speeders and the slower drivers by allowing slight limitations on some people’s rights, while enabling enjoyment on behalf of others. The Internet needs some regulation so that it is an information highway that all users can travel upon freely and safely.

Without assurance of some level of privacy protection, the benefits of the technology of the Internet begin to dwindle. For example, the ability to disseminate privileged or secure information via computer network extends huge benefits of convenience as well as economizes time, money and resources. Prior to computer communications, a document vital to national security or a company’s stockholders had to be transported by someone holding some type of trusted position. Often, in the military, an officer would transport a document by hand, flying to another state or country. In the computer age, that document can be encrypted and sent via computer in a matter of seconds. The possibility that a document could be intercepted, decoded, read and widely disseminated, mandates considering a return to the past means of transporting information, despite its huge monetary cost or by protection through FCC regulation. The consideration increases particularly when the cost-benefit analysis includes national security.

IV. CONCLUSION

Increased technology often creates new, unforeseen problems. Merely applying the Bill of Rights to the electronic world of Cyberspace is insufficient. Until the legislature truly understands the complex highway of computer technology, the current laws will remain inadequate.

The need for some method of securing systems is undeniable. However, preventing repeat abusive governmental power such as that evidenced in *Steve Jackson Games* must be balanced with the government’s legitimate interest in the ability to protect Cyberspace from rampant crime.

Privacy protections such as the Clipper Chip will be a long time coming. In the meantime, the law and the agencies writing and implementing it must move full speed ahead to catch up with current technology and protect the privacy that American citizens hold so dear.