November/December 2001

Michigan COMPUTER LAWYER

Editor
Paul J. Raine
praine@home.msen.com

http://www.michbar.org/sections/computer/

State Bar of Michigan Computer Law Section

Our Section … By Any Other Name

Sometimes ambiguity is a good thing. When a senior partner invites a new associate to a dinner party but serves a poorly prepared meal, it is not a time for the associate to be completely candid. When asked how he liked the meal, "interesting" or "original" are much more diplomatic responses. They apply equally whether the associate liked the meal or not and, therefore, avoid the awkwardness that would follow a precise answer to the partner's question. Ambiguity can serve more noble purposes as well. It can make a statement more comprehensive. For example, the World Wildlife Fund is concerned with a broader range of animals than is Trout Unlimited (although I recommend them both as worthy causes). Your council is struggling to determine whether "Computer Law Section" is a good use of ambiguity or whether the section should change its name. Suggested new names include "Computer and Information Technology Section," "Computer and Internet Law Section" or "Cyberspace and Computer Law Section."

No Title-Object Clause requires the section's name to reflect its purpose but it is probably a good idea. Attorneys or others with whom we deal should gain some sense of our substantive focus from the section's name. That said, there can be little doubt that the name "Computer Law Section" is ambiguous. What precisely is "Computer Law"? The term applies equally to copyright protection for software as it does to e-commerce agreements or information technology licenses or Internet privacy issues. We have presented this broad a range of topics at our Spring networking luncheons, annual meeting programs and recent council meetings.

Fundamentally, section members' interests and expectations determine the section's focus. National organizations may adequately inform you about protecting software with patents but not about the peculiar impact of Michigan statutes on e-commerce. On the other hand, members may rely on the section to present local seminars on topics of interest even if there are no particularly unique aspects to the topics under Michigan law. These are the expectations your council must gauge to determine the section's purpose.

There are other considerations, of course. Continuity is valuable. We will not change the name if our members and fellow attorneys already associate a clear understanding of our mission with the name "Computer Law Section." Your input on this decision is very important. I urge you to contact Gregory L. Ulrich (gulrich@cmda-law.com), chairperson of the committee investigating the name change, with your thoughts, suggestions and concerns. I am interested in them as well.

Jeffrey G. Raphelson, Chairperson Computer Law Section
100 Renaissance Center, 34th Floor
Detroit, Michigan 48243
jraphelson@bodmanlongley.com

3 Carnivore: Devouring Our Right to Privacy

11 Seminar Reimbursement Program

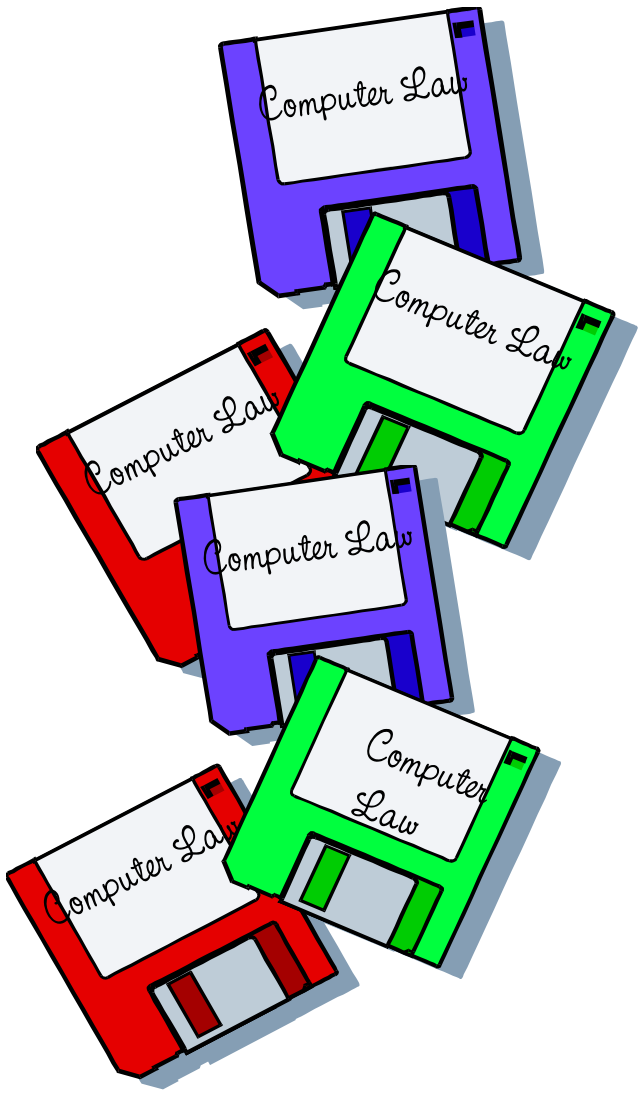
Michigan Computer Lawyer **is published bi-monthly. If you have an article you would like considered for publication, send a copy to:**

Paul J. Raine
Attorney at Law
PO Box 99773
Troy, MI 48099
praine@home.msen.com

Statement of Editorial Policy

The aim and purpose of the Michigan Computer Law Section of the State Bar of Michigan is to provide information relative to the field of computer law, and other information that the section believes to be of professional interest to the section members.

Unless otherwise stated, the views and opinions expressed in the Michigan Computer Lawyer are not necessarily those of the Computer Law Section, or the State Bar of Michigan.



Computer Law Section

Carnivore: Devouring Our Right to Privacy

By Nina Korkis --Second Place Winner, Ed Langs Writing Competition 2000

Nina Korkis is now an assistant prosecuting attorney for the Wayne County Prosecutor's Office.

The Internet has become a necessity and permanent fixture in most workplaces, schools, and libraries. Millions of people use the Internet to access electronic mail (e-mail), shop, or just surf the World Wide Web. The growing reliance on computers and the Internet has vastly increased the potential for government to use electronic surveillance to invade its citizens' private lives.[1] Anytime individuals use the Internet, they are leaving behind a series of electronic footprints that can be tracked and monitored by the government. As a result, individuals are losing the ability to physically lock away sensitive information from government eyes.[2]

With the advent of the digital age, old crimes are being committed through new means, which poses challenges to law enforcement agencies trying to carry out their duties. However, a system such as Carnivore cannot be squared with the Fourth Amendment or the Electronic Communications Privacy Act (ECPA), which was adopted to implement Fourth Amendment principles in the context of electronic surveillance. Carnivore violates the essence of the Fourth Amendment, which is to protect individual privacy rights against general searches by the government, into the private communications of innocent persons.

Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[3]

CARNIVORE

A. What is Carnivore?

The Federal Bureau of Investigation (FBI) created Carnivore in February 1997 under the name Omnivore.[4] In June 1999, Omnivore was replaced by a system called Carnivore, which is specialized software that runs on Microsoft Windows.[5] Carnivore is a "network sniffer" or "black box" which can intercept large volumes of e-mail and other forms of electronic communication passing through an Internet Service Provider's (ISP) network once plugged directly into an ISP's data center.[6] Theoretically, Carnivore can scan millions of e-mail messages per second, processing as much as six gigabytes (6,000 megabytes) of data every hour.[7] In practice, the FBI contends that Carnivore scans the subject lines and headers of e-mail messages to identify communications among selected individuals who are the targets of a criminal investigation.[8]

The public first learned of Carnivore when an attorney for Earthlink Inc. (Earthlink), an ISP, informed the House Judiciary Committee that the FBI was forcing the company to install Carnivore on its network to execute court-ordered surveillance of criminal suspects.[9] Earthlink allowed the FBI to install Carnivore at a network test site and it caused network performance problems and crashes.[10] Unfortunately, the FBI would not allow Earthlink to examine Carnivore to resolve whether its capturing of e-mail and other traffic violated the privacy rights of its customers.[11] Therefore, due to network problems and the serious threat to the privacy rights of its subscribers, Earthlink refused to install Carnivore on its network.[12] The FBI's reluctance to disclose information about Carnivore has fueled nationwide controversy over the device.

B. What are Carnivore's technical capabilities?

As a result of the public uproar over Carnivore, on July 24, 2000 and September 6, 2000, the United States Senate heard testimony about Carnivore from various people, including law enforcement officials, civil liberties groups, ISP owners, and law professors. The testimony was intended to furnish the public with technical details concerning Carnivore, as well as its constitutional implications.

Donald M. Kerr, Assistant Director of the FBI, testified that "Carnivore is a very effective and discriminating special purpose electronic surveillance system . . . which the FBI has developed to carefully, precisely, and lawfully conduct electronic surveillance of electronic communications occurring over computer networks."[13] Mr. Kerr further explained how Carnivore's special "filtering" process operates in stages.[14] First, Carnivore filters a portion of an ISP's high speed network traffic (specifically binary code).[15] Binary code are the streams of 0's and 1's that flow through an ISP's network.[16] Carnivore scans millions of 0's and 1's to find out whether the particular identifying information on a criminal subject is available.[17] Second, if the criminal subject's identifying information is detected, that information alone is segregated for additional

continued on page 4

filtering or storage.[18] Theoretically, all of the other millions of 0's and 1's associated with other (innocent) communications "are instantaneously vaporized after that one second."[19] Third, after "exclusively" filtering the criminal subject's information for further processing, Carnivore determines, as required by the wording of the court order, "if it is supposed to comprehensively collect communications content . . . or, alternatively, whether it is only to collect pen register or trap and trace transactional and addressing information."[20] Mr. Kerr assured the Senate that all of the filtering and processing occurs in the Carnivore "box" and that "what finally reaches the hands of FBI personnel in every case is simply and only that particular information lawfully authorized by the court order – and no more."[21] Finally, for evidentiary purposes, Carnivore is also designed to keep records of the information it collects.[22]

In addition, Mr. Kerr stated that ISP's should not be fearful about Carnivore's use with their networks.[23] According to Mr. Kerr, "Carnivore is only installed in that small segment of the computer network through which the criminal subject's communications traffic will pass."[24] Carnivore is purportedly connected to the network by a bridging device that makes it physically impossible for it to transmit into the network.[25] Furthermore, Carnivore is only attached to the network after consultation with, and after obtaining the agreement and assistance of, technical personnel from the ISP.[26]

Testimony from Peter William Sachs, an attorney and president of a Connecticut-based ISP, was also presented before the House of Representatives on July 24, 2000 concerning Carnivore and its capabilities.[27] Mr. Sachs explained how e-mail works to better understand the controversy surrounding Carnivore.[28] Initially, "when an email message leaves a sender's computer, it is broken up into unintelligible pieces of data called packets."[29] Next, "each packet knows where it came from and how to get where it's going because each packet contains the addresses of the sender and of the recipient, just like an envelope."[30] Finally, the packets navigate the Internet and arrive at the recipient's ISP.[31] Upon arrival at the ISP, "the packets are reassembled by mail server software into a useful form and stored in the recipient's mailbox until the recipient retrieves it."[32]

Mr. Sachs disagreed with Mr. Kerr's claim that "Carnivore has the surgical ability to intercept only those messages that are the subject of a lawful order while ignoring the rest."[33] Mr. Sachs asserts that this is possible only if Carnivore can detect and then monitor only the IP[34] address assigned to the target during a particular online session.[35] Furthermore, to accomplish its task, "Carnivore would have to continually monitor all logins to find the one login it is looking for."[36] According to Mr. Sachs, "intercepting all logins is the functional equivalent of intercepting the telephone number of every call initiated by every customer of a particular telephone carrier."[37] Mr. Sachs also made it clear that if the FBI wanted to accomplish its task, it would have to actually view each message to see if it contained incriminating information.[38] Mr. Sachs confessed that the secretive nature of the Carnivore system prevented him from explaining the precise deficiencies in the system and that "exactly what Carnivore does remains a mystery."[39] Therefore, because Carnivore is so intrusive and poses a serious threat to the privacy rights of ISPs and Internet users, it should be examined in light of Fourth Amendment principles.[40]

Civilization is the progress toward a society of privacy.[41]

II. THE FOURTH AMENDMENT

A. A Brief Overview of the Fourth Amendment

During the pre-Revolutionary War period, English officers were granted unfettered discretion, through the use of general warrants, to search anywhere and anytime they pleased for goods imported in violation of British tax laws.[42] It is generally well accepted that "indiscriminate searches and seizures conducted under the authority of general warrants were the immediate evil that motivated the framing and adoption of the Fourth Amendment."[43] Thus, as a result of the unreasonable law enforcement practices employed by English officers, the Fourth Amendment was adopted, which states: "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."[44] As technology advanced, government officials began employing new types of sophisticated eavesdropping devices to aid in their law enforcement duties. Thus, courts were forced to re-examine Fourth Amendment principles in light of new technological advances which posed a threat to individual privacy rights.

B. The Fourth Amendment and Electronic Surveillance

In *Olmstead v. United States*,[45] the court promulgated Fourth Amendment principles in the context of wire-tapping phone conversations. The issue before the Court was whether the use of evidence of private telephone conversations, intercepted by wire-tapping, amounted to a violation of the Fourth and Fifth Amendments.[46] The defendant was convicted of leading a conspiracy to violate the National Prohibition Act.[47] Federal officers obtained information about the conspiracy by intercepting messages on the telephones of the conspirators.[48] The Court stated that the historical purpose of the Fourth Amendment "directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers and his effects; and to prevent their seizure against his will."[49] In affirming the defendant's convic-

tion, the Court held that because there was no search of anything material or tangible, or any kind of actual physical trespass upon the property of the defendant, there was no violation of the Fourth Amendment.[50]

After almost forty years, the Court reversed *Olmstead*[51] in *Katz v. United States*.[52] In *Katz*, the defendant was convicted of violating 18 U.S.C. sec. 1084, which criminalized interstate transmission by wire communication of bets or wagers.[53] The defendant was seen placing calls from three public telephone booths on an almost daily basis.[54] FBI agents planted microphones on the outside of the public telephone booths used by the defendant.[55] The FBI obtained records of the defendant's end of a series of phonecalls, which revealed that the defendant was engaged in interstate gambling.[56] In affirming the defendant's conviction, the court of appeals held that there had been no violation of the Fourth Amendment because there was no physical entrance into the area occupied by the defendant.[57] However, the United States Supreme Court disagreed with the reasoning of *Olmstead* and the court of appeals and stated, "the Fourth Amendment protects people, not places."[58] The Court rejected the government's argument that the defendant did not enjoy an expectation of privacy in the phone booth because it was partly made of glass and was visible to those outside.[59] Instead, the Court stated that what the defendant "sought to exclude when he entered the booth was not the intruding eye – it was the uninvited ear. [The defendant] did not shed his right to do so simply because he made his calls from a place where he might be seen."[60] The Court held that "the government's activities in electronically listening to and recording the [defendant's] words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[61] Thus, a defendant raising a challenge to a government search or seizure must show that he or she: (1) has a subjective expectation of privacy, and (2) the expectation is one that society accepts as objectively reasonable.[62]

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986 (ECPA)

A. Pre-ECPA Principles

As a result of the United States Supreme Court's decision in *Katz*,[63] Congress recognized the need to enhance the protection of privacy rights by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[64] With the passage of Title III, Congress intended to effectuate two central purposes: (1) protecting the privacy of wire and oral communications, and (2) outlining the proper circumstances and conditions under which an interception of wire and oral communications may be authorized.[65] However, with the advent of new technology, the absence of protection of privacy interests in electronic communications created serious problems, such as electronic espionage and computer hackers.[66]

In 1986, Congress broadened Title III to include protection of "electronic communication" and renamed it the Electronic Communications Privacy Act (ECPA).[67] According to a Senate Report,[68] the ECPA was designed to make sure the law advanced with technology and to ensure the continued vitality of the Fourth Amendment.[69] The ECPA created the two most important statutory safeguards against unwanted searches of electronic communications and data:[70] Title I[71] and Title II,[72] as codified in Title 18 of the United States Code (Crimes and Criminal Procedure).

B. ECPA Principles

Title I of the ECPA regulates the interception and disclosure of wire,[73] oral,[74] or electronic communications.[75] The ECPA does not require that communications be transmitted via common carrier.[76] Under the ECPA, "electronic communication" is defined 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."[77]

Electronic communications on the Internet fall within this definition because the Internet affects interstate or foreign commerce. Title I protects only the content of a communication, not the existence of a communication.[78] Thus, law enforcement officials "can lawfully determine the identities of the computer systems that one accesses, and can monitor the recipients and sources of one's electronic mail, so long as the contents of the communications are not intercepted."[79] The ECPA only protects private communications.[80] Therefore, electronic communications, such as chat rooms, that are readily accessible to the public, are not protected by the ECPA. Furthermore, Title I applies only to the interception of transmissions.[81]

Title II of the ECPA affords statutory protection to stored wire or electronic communications from unauthorized access.[82] An individual or an entity violates Title II by intentionally accessing or exceeding his or her authorization to use an electronic communication facility, and then obtaining, altering or preventing authorized access to a stored electronic communication.[83] The most crucial aspects of Title II "prohibit private citizens from gaining unauthorized access to stored electronic communications and enumerate specific procedural requirements for a government entity to gain access to stored electronic communications."[84] Law enforcement officials may gain access to electronic communications that have been stored less than 180

Continued on page 6

days only when approved by a valid warrant.[85] Subsequently, if an electronic communication is stored longer than 180 days, law enforcement officials may obtain access to it via grand jury, trial subpoena, or court order supported by a reasonable belief that the contents of the communication are relevant to a criminal investigation.[86] In addition, Title II "prohibits the nonconsensual disclosure to government entities of information other than the contents of communications to the government, unless compelled by subpoena, warrant, or court order."[87] Title II protects information such as the identities of e-mail subscribers, the types of services the subscribers use, and where a subscriber is physically located.[88] Thus, stored electronic communications enjoy more statutory protection than electronic communications that are in transit.

LEGAL ISSUES IN CYBERSPACE

A. The Internet

The Internet is not a tangible entity, "but rather a giant network which interconnects innumerable smaller groups of linked computer networks."[89] The Internet was created in 1969 by the Advanced Research Project Agency (ARPA), and was named ARPANET.[90] Initially, it was a defense-related research tool used mainly by the military and university laboratories.[91] It later evolved far beyond its original intended use to become a global communications medium for people all over the world.[92] "No single entity . . . administers the Internet . . . There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet."[93] The most common method of accessing the Internet is to use a "personal computer with a modem to connect over a telephone line to a larger computer or computer network that is directly or indirectly connected to the Internet."[94]

B. Electronic Mail

Once connected to the Internet, individuals have a variety of different ways to communicate with each other, most notably, using electronic mail (e-mail) and chat rooms.[95] E-mail is a form of private communication in which the sender of an e-mail message uses a keyboard to type a message into a computer and a modem transmits the message over a telephone line to a recipient through the Internet.[96] Sending e-mail is similar to sending a first class letter.[97] Like postal mail, "e-mail on the Internet is not routed through a central control point, and can take many and varying paths to the recipients."[98] However, unlike postal mail, e-mail "generally is not sealed or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)."[99] Generally, with e-mail, messages are transmitted for people to read or access at a later time. Chat rooms, however, provide "real time communication" whereby individuals on the Internet can engage in immediate communication with other people on the Internet.[100] Chat rooms are analogous to a telephone party line, using a computer and keyboard rather than a telephone.[101]

One example of an ISP, which provides such services, is America Online (AOL). AOL is a private company that charges monthly fees based upon the number of hours one spends online.[102] As part of the registration process, AOL requires the subscriber to "provide his or her name, address, and billing information, and an account is created for that individual on the system."[103] The subscriber then must choose at least one screen name, but has the option of choosing up to five, which becomes the subscriber's identification on–line.[104] No two subscribers will have the same screen name.[105] The subscriber also must use a password to access the system.[106] In addition, "all e-mail is stored in AOL's central computer for access and retrieval for 5 weeks to allow for the possibility of vacations and extended trips, and then messages are purged from the system."[107] The question of whether individuals enjoy a reasonable expectation of privacy in e-mail messages has been debated by courts. While there have not been many cases specifically addressing this issue, some courts have found that e-mail messages enjoy Fourth Amendment protection.

C. Cases Finding A Reasonable Expectation of Privacy In E-mail Messages

In *United States v. Maxwell*,[108] the defendant, a Colonel in the U.S. Air Force, was convicted of the communication of indecent language, knowingly distributing obscene material, and knowingly transporting or receiving child pornography in interstate commerce.[109] In 1991, an AOL subscriber reported to the press that child pornography was being distributed on AOL.[110] This report ultimately resulted in an FBI investigation, which included securing a warrant to search AOL's computer bank.[111] After the FBI received information from AOL and reviewed its contents, it was discovered that the defendant was involved in the investigated activities.[112] The FBI then contacted the Air Force of Special Investigations (AFOSI), which conducted its own investigation of the defendant using all of the seized material from the FBI.[113] AFOSI agents seized defendant's Apple Macintosh computer from his quarters.[114]

One of the main issues before the court was whether defendant, as a subscriber to AOL, possessed a reasonable expectation of privacy in the e-mail messages he sent and/or received, which were stored in AOL's computers.[115] In determining whether defendant had a reasonable expectation of privacy, the court distinguished AOL from the Internet and stated that with AOL "e-mail messages are afforded more privacy than similar messages on the Internet, because they are privately stored for retrieval on AOL's centralized and privately-

owned computer bank located in Vienna, Virginia."[116] The court also asserted that when an individual sends messages on the computer, the Fourth Amendment expectation of privacy diminishes on a sliding scale.[117] For example, "the more open the method of transmission, such as the 'chat room,' the less privacy one can reasonably expect."[118] Drawing from examples of mediums in which people have a reasonable expectation of privacy, such as sending first-class mail and making a telephone call, the court acknowledged that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[119] The court found that the possibility a "hacker" might intercept an e-mail message did not diminish the legitimate expectation of privacy an e-mail message should receive.[120] Thus, the court ultimately held that an expectation of privacy exists in e-mail transmissions made on the AOL service.[121]

United States v. Charbonneau[122] also involved an FBI investigation into child pornography on the Internet. In this case, FBI agents would access AOL, specifically chat rooms, and pose as pedophiles.[123] The agents observed a user named "Charbyq" sending child pornography, and obtained a search warrant to identify the user as the defendant.[124]

One of the issues before the court involved a motion to suppress any statements made by defendant while on the Internet using AOL.[125] Citing *Maxwell*, the court stated "defendant possessed a limited reasonable expectation of privacy in the e-mail messages he sent and/or received on AOL."[126] However, unlike the defendant in *Maxwell*, the defendant here sought to suppress all of the statements he made in AOL chat rooms.[127] The court stated that when defendant used the AOL chat rooms, he ran the risk of "chatting" with an undercover agent, and that such statements are not protected by the Fourth Amendment.[128] In denying the defendant's motion to suppress, the court stated that "defendant could not have a reasonable expectation of privacy in the chat rooms."[129]

Maxwell and *Charbonneau* may not be the final authority on whether an expectation of privacy exists in e-mail messages communicated over an ISP. However, the reasoning of both cases is highly persuasive, and should serve as a benchmark for future courts that are confronted with this issue. Both cases demonstrate that society is willing to accept an expectation of privacy in their e-mail messages.

CARNIVORE THREATENS PRIVACY RIGHTS

A. Carnivore Performs Illegal Searches in Violation of the Fourth Amendment

Carnivore is an Internet wiretapping device that violates the rights of all individuals using the services of an ISP. Because Carnivore "intercepts all communications coming from or going to an ISP, including communications outside the scope of the court order, it amounts to an unwarranted intrusion upon [the] privacy rights of non-targeted persons."[130] The searches conducted using Carnivore are much like general warrants because they are broad and abusive, and are led by executive officials with unlimited discretion.

At least two courts have found that an expectation of privacy exists in e-mail transmissions made on an ISP's network. The sending of an e-mail message is often compared with sending a first class letter. This analogy is useful because it illustrates the level of privacy individuals attribute to their e-mail communications. The fact that individuals must use a password to send or receive e-mail also demonstrates the extent to which individuals will go to keep their e-mail private. Carnivore simply cannot be squared with the Fourth Amendment because it gives law enforcement officials carte blanche authority to access the e-mail communications of innocent people.

B. Carnivore Violates the ECPA

1. The ECPA Protects E-Mail Messages

Although the ECPA does not specifically mention "e-mail," the statutory language provides protection for "electronic communication." The legislative history of the statute indicates that the legislature anticipated that the ECPA protections against interception and disclosure would also apply to e-mail messages.[131] The stringent ECPA requirements governing wiretaps apply to Carnivore when it is used to capture the content of e-mail messages or other electronic communications.[132] Furthermore, both the subject line and text of an e-mail message are content, which law enforcement officials may intercept only under a wiretap order.[133]

2. Law Enforcement Officials Should Be Prohibited From Installing Carnivore on an ISP's Network Under the Low Threshold Required For Pen Registers and Trap and Trace Devices

Unlike a conventional wiretap, pen register,[134] or trap and trace device,[135] Carnivore gives the FBI access to **all** of the traffic over an ISP's network, instead of targeting specific communications pursuant to a valid court order. The FBI claims that Carnivore can be used as the Internet functional equivalent of a pen register or trap and trace device that provides information about the source or destination of a telephone call.[136] However, the address and header information contained in an e-mail message provides far more detail about the interests of the person sending the e-mail than a dialed number on a telephone.[137]

The law prescribes a far lesser threshold for obtaining a pen register order than it does other forms of electronic surveillance.[138] The ECPA provides that a court "shall enter an ex

Continued on page 8

parte order authorizing the installation and use of a pen register or trap and trace device" where a law enforcement officer certifies that the "information likely to be obtained is relevant to an ongoing criminal investigation."[139] The reason for this is that more limited information is acquired from a pen register or trap and trace device. However, an order to intercept the content of electronic communications requires a showing of probable cause that the target has committed a specific felony outlined in the statute.[140] The judge might grant a request for such an interception if there is a showing of probable cause, an indication that normal investigative procedures have failed, the identity of the person whose communications are to be intercepted, and the particular type of communication sought to be intercepted.[141]

Law enforcement officials are obtaining ex parte orders for the installation of Carnivore at various ISPs under the low standards required for a pen register or trap and trace device on a showing that a specified communication is relevant to an ongoing criminal investigation.[142] In other words, law enforcement officials have broad leeway to seek such an order without the probable cause required for searches under the Fourth Amendment. This is very problematic because the information revealed by Carnivore is much more invasive than the telephone numbers revealed by a pen register.[143] Pursuant to a Carnivore search of all the traffic over an ISP's network, the government "has access to the identity of the recipient and sender of the specified communication, and, in the case of URL addresses, to search the terms that may have been entered in an Internet search."[144] Although the United States Supreme Court has held that "citizens have no reasonable expectation of privacy in information, like telephone numbers, that they have voluntarily turned over to the phone company and that they expect the phone company to record,"most citizens probably would not feel the same about their personal records of Internet searches and reading habits.[145]

3. The Pen Register and Trap and Trace Concepts in the ECPA Are Ill-Suited for the Internet

The pen register and trap and trace concepts set forth in the ECPA simply do not fit well in cyberspace.[146] The pen register and trap and trace rules under the ECPA do not seem to apply to ISPs and the Internet.[147] Just from reading the definitions above, it is clear that Congress intended for these provisions of the ECPA to refer only to devices used in connection with telephones.[148] Even though information in e-mail is transmitted over telephone lines, this does not transform the facilities of an ISP, such as AOL, into "telephone lines."[149] Therefore, pen registers, trap and trace devices, and Carnivore are "installed on the data network of an ISP, not on a telephone line, and the information which may be intercepted is not limited to that transmitted over a single subscriber line."[150] Because the Internet runs on a packet-switched network,[151] instead of a circuit-switched network,[152] Carnivore's interception of packetized information allows the government to receive both identifying information and content.

C. Carnivore is Unnecessary

Carnivore is unnecessary because an ISP can easily supply the FBI with all of the information it needs in a timely, accurate and efficient manner, and, most importantly, without imposing upon the privacy rights of those who are not the subject of the investigation.[153] According to Peter William Sachs, owner of a small ISP in Connecticut, "an ISP can intercept any subscriber's incoming and outgoing email messages to the exclusion of all others."[154] In fact, ISPs can perform such a service without a specialized computer system or special programming skills.[155] To support his statements, Mr. Sachs asked one of his system engineers to create a program that could intercept all of his electronic communications on the Internet.[156] According to Mr. Sachs, "in less than an hour, all of the words [he] sent or received via email appeared on [the system engineer's] computer in plain, legible text."[157] In addition, "an ISP can easily exclude all communications that are outside the scope of the court order without ever looking at them because an ISP can and does detect each login as part of its internal operation."[158] Using this method, only the messages of the target are intercepted and unwarranted intrusions are avoided altogether.[159]

VI. CONCLUSION

The Internet will remain a powerful tool for the future. The relative inexpensiveness and simplicity of sending and receiving e-mail messages will secure e-mail as a leading communication tool in today's society. Carnivore, which is capable of scanning millions of e-mail messages per second, purportedly retains only the messages of a specified target, yet the entire process takes place without the scrutiny of both ISPs and courts. This kind of unbridled discretion from government officials is precisely the type of abuse the framers of the Fourth Amendment and the ECPA sought to prevent. The FBI should release Carnivore's source code so that it may be examined in light of the Fourth Amendment and the ECPA.[160] Until the FBI divulges significant information about Carnivore, individuals should use encryption[161] to protect the privacy of their e-mail messages.

Endnotes

1 Raphael Winick, Article, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J. Law & Tec. 75, 76 (1994).
2 Winick, *supra* note 1, at 76.
3 Olmstead v. United States, 277 U.S. 438, 473 (Brandeis, J., dissenting).
4 Ann Harrison, *Privacy Group Critical of Release of Carnivore Data* (visited Nov. 6, 2000) *<http://www.computerworld.com/cwi/story>*.

5 *Id*.
6 Bradley Mitchell, *Carnivore, Sniffers, and You* (visited Nov. 13, 2000) <*http://www.compnetworking.about.com*>.
7 *Id*.
8 *Id*.
9 Ann Harrison, *Privacy Group Critical of Release of Carnivore Data* (visited Nov. 6, 2000) <*http://www.computerworld.com/cwi/story*>.
10 *Id.*
11 *Id.*
12 *Id.*
13 *Electronic Surveillance*: *Testimony on Carnivore Before the United States Senate, The Committee on the Judiciary*, *reprinted in* 2000 WL 1268432 (F.D.C.H.), (statement of Donald M. Kerr, Assistant Director Federal Bureau of Investigation). Carnivore has purportedly only been used 25 times in the last two years. *Id*.
14 *Id.*
15 *Id.*
16 *Id.*
17 *Id.*
18 *Id.*
19 *Supra* note 13.
20 *Id.*
21 *Id.*
22 *Id.*
23 *Id.*
24 *Id.*
25 *Id.*
26 *Id.*
27 *Carnivore and the Fourth Amendment*: *Testimony before the House of Representatives, on the Judiciary*, *reprinted in* 2000 WL 1073250 (F.D.C.H.) (statement of Peter William Sachs, President of ICONN, LLC and licensed attorney from Connecticut).
28 *Id.*
29 *Id.*
30 *Id.*
31 *Id.*
32 *Id*. This information is stored, if at all, on the recipient's computer. *Id*.
33 *Supra* note 27.
34 An Internet address is known as an IP address and every computer connected to the Internet has a unique IP address. *Id*.
35 *Id.*
36 *Id.*
37 *Id*. The use of e-mail has become as common a communication tool as the telephone. This year alone, it is estimated that over 6 trillion e-mail messages will pass through e-mail servers in the United States. *Id*.
38 *Id.*
39 *Id*. Mr. Sachs stated that his conclusions were based on his knowledge of ISP operations and the FBI's claims as to the capabilities of Carnivore. *Id*.
40 *Id*. An "independent" team is currently conducting a technical review of Carnivore. *See ACLU Says Government Stacked Deck in Selection of Team to Review "Carnivore" Cyber-Tapping System*, (visited October 12, 2000) <http://www.aclu.org/features>.
41 AYN RAND, THE FOUNTAINHEAD 7 (1943).
42 Payton v. New York, 445 U.S. 573, 585 (1980), (citing Boyd v.U.S., 116 U.S. 616, 625).
43 Id. at 583.
44U.S. CONST. Amend. IV.
45 *Olmstead*, 277 U.S. at 438.
46 *Id*. at 455.
47 *Id*. at 455-56.
48 *Id*. at 456.
49 *Id*. at 463.
50 *Id*. at 466.
51 S*upra* note 3.
52 389 U.S. 347 (1967).
53 *Id*. at 348.
54 *Id.*
55 *Id*. at 349.
56 *Id*.
57 *Id*. at 348-49.
58 *Katz*, 389 U.S. at 351.
59 *Id*. at 352.
60 *Id*.
61 *Id*. at 353.
62 California v. Greenwood, 486 U.S. 35, 39 (1988).
63 S*upra* note 51.
64 18 U.S.C. sec. 2510 et seq.
65 United States v. Cianfrani, 573 F.2d 835, 855 (3rd Cir. 1978).
66 Tatsuya Akamine, Notes and Comment, *Proposal For A Fair Statutory Interpretation: E-Mail Stored In A Service Provider Computer Is Subject To An Interception Under The Federal Wiretap Act*, 7. J.L. & Pol'y 519, 533 (1999).
67 18 U.S.C. sec. 2510 et seq.
68 S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.A.A.N. 3555, 3559.
69 Akamine, *supra* note 59, at 529.
70 Winick, *supra* note 1, at 90.
71 18 U.S.C. sec. 2511.
72 18 U.S.C. sec. 2701.
73 18 U.S.C. sec. 2510(1) defines wire communication as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . . ." *Id*.
74 18 U.S.C. sec. 2510(2) defines oral communication as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *Id*.
75 18 U.S.C. sec. 2510(12).
76 Winick, *supra* note 1, at 90.
77 18 U.S.C. sec. 2510(12).
78 Winick, *supra* note 1, at 93.
79 Winick, *supra* note 1, at 93-94.
80 Winick, *supra* note 1, at 94.
81 Winick, *supra* note 1, at 95.
82 18 U.S.C. sec. 2701.
83 18 U.S.C. sec. 2701.
84 Winick, *supra* note 1, at 96. *See* 18 U.S.C. 2701(a).
85 Winick, *supra* note 1, at 96. *See* 18 U.S.C. 2703.
86 Winick, *supra* note 1, at 96-97.
87 *See* 18 U.S.C. 2703.
88 Winick, *supra* note 1, at 97.
89 ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. PA 1996).
90 *Id.* at 831.
91 *Id*.
92 *Id*.
93 *Id.* at 832.
94 *Id*.
95 *ACLU*, 929 F.Supp. at 833.
96 *Id*.
97 *ACLU*, 929 F. Supp. at 834.
98 *Id*.
99 *Id*.
100 *Id*. at 835.
101 *Id.*
102 United States v. Maxwell, 45 M.J. 406, 410 (C.A.A.F. 1996).
103 *Id*. at 411.
104 *Id.*
105 *Id.*
106 *Id.*
107 *Id*. at 412.
108 United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).
109 *Id*. at 410. The defendant was specifically convicted under Article 134, Uniform Code of Military Justice, 10 U.S.C. sec. 934, 18 U.S.C. sec. 1465, and 18 U.S.C. sec. 2252.

Continued on page 10

110 *Id.* at 412.
111 *Id.* at 412-13.
112 *Id.* at 414.
113 *Id.* Defendant purchased all of his computer hardware and software with his personal funds and he only used the service while at home and off-duty. *Id.*
114 Maxwell, 45 M.J. at 414.
115 *Id.* at 416.
116 *Id.* at 417.
117 *Id.*
118 *Id.*
119 *Id.* at 418.
120 *Maxwell*, 45 M.J. at 418.
121 *Id.*
122 979 F.Supp. 1177 (S.D. OH 1997).
123 *Id.* at 1179.
124 *Id.*
125 *Id.* at 1183.
126 *Id.* at 1184.
127 *Id.* at 1185.
128 *Charbonneau*, 979 F. Supp. at 1184-85. *See* United States v. Hoffa, 385 U.S. 293 (1966) (holding that statements made to undercover agents are not protected by the Fourth Amendment).
129 *Id.* at 1185.
130 *Supra* note 27.
131 *See* S.REP. NO. 99-541, at 8 (1986), *reprinted in* 1986 U.S.C.A.A.N. 3555, 3568 (stating that although the ECPA does not directly address e-mail messages, the scope of the statute covers e-mail, digitized transmissions, and video teleconferences).
132 *Electronic Surveillance and Privacy in the Digital Age*: *Hearing on the Carnivore Controversy*, *Senate Judiciary Committee*, *reprinted in* 2000 WL 1268431 (F.D.C.H.) (statement of Sen. Patric Leahy).
133 *Id.*
134 A pen register is a device that records the numbers that are dialed from a telephone. *Carnivore and the Fourth Amendment*, *The Fourth Amendment and the Internet*: *Testimony before the House of Representatives*, *reprinted in* 2000 WL 1073248 (F.D.C.H.) (statement of Robert Corn-Revere, Adjunct Law Professor, licensed attorney).
135 A trap and trace device is used to discover the number of origin of a telephone call. *Id.*
136 *Id.*
137 *Id.*
138 *Id.*
139 18 U.S.C. sec. 3123(a).
140 See 18 U.S.C. sec. 2516, 2518.
141 18 U.S.C. sec. 2518.
142 *Supra* note 134. *See* 18 U.S.C. 3123(a).
143 *Electronic Surveillance*, *The Fourth Amendment and the FBI's Carnivore Program*: *Testimony before the Senate Judiciary Committee*, *reprinted in* 2000 WL 1268435 (F.D.C.H.) (statement of Jeffrey Rosen, Professor, George Washington University Law School).
144 *Id.*
145 *Id.*
146 *Supra* note 134.
147 *Id.*
148 *Id.* See 18 U.S.C. sec. 3127(3).
149 *Id.*
150 *Id.*
151 *Supra* note 134. "In a packet-switched network, there is no single, unbroken connection between sender and receiver. Instead when information is sent, it is broken into small packets, sent over many different routes at the same time, and then reassembled at the receiving end." *Id.*
152 "In a circuit-switched network, after a connection is made (as with a telephone call, for example), that part of the network is dedicated only to that single connection." *Id.*
153 *Supra* note 27.
154 *Id.*
155 *Id.*
156 *Id.*
157 *Id.*
158 *Id.*
159 *Id.*
160 *See* EPIC v. DOJ, Memorandum Opinion (D.C. Cir. 2000) (where the Electronic Privacy Information Center (EPIC) has asked a federal judge to order the FBI to immediately release more information about Carnivore). To download information about the lawsuit and view documents the FBI has currently released about Carnivore, go to *<http://www.epic.org/privacy/carnivore.html>*.
161 *See* David L. Gripman, Article, *Electronic Document Certification: A Primer On the Technology Behind Digital Signatures*, 17 J. Marshall J. Computer & Info. L. 769, 774 (1999). "An encryption software takes a readable message called "plaintext" and runs it through a mathematical algorithm to scramble the message into unreadable "ciphertext." The ciphertext message is sent to a receiver who uses a "key" to decrypt the ciphertext back into readable plaintext. Anyone who intercepts the message will see unreadable gibberish and without the key, will be unable to unscramble the ciphertext. Thus, encryption allows private and confidential communications via email between parties over the Internet."

Don't forget to check out our Section Website at *www.michbar.org!*

Computer Law Section
Seminar Reimbursement Program

If you're a member of the Computer Law Section, you may be eligible to receive reimbursement for the cost of attending a computer law related seminar. If approved, you need only agree to submit a written article summarizing the seminar for publication in the section's newsletter and make an oral presentation at a section meeting.

To apply for reimbursement under this program, at least 4 weeks before the seminar send the following information along with your request for reimbursement to one of the reimbursement program coordinators, David Syrowik at *dsyrowik@brookskushman.com* **or Kimberly Paulson at** *paulson@millercanfield.com***:**

1. **Your name, address, phone number, and e-mail address.**

2. **The name, date, location, and description of the seminar you wish to attend, as well as its cost. Please retain a copy of the seminar's brochure to submit to the Council for approval.**

3. **Identification of the portions of the seminar you intend to attend and report on.**

Within two weeks of your request, the Council of the Computer Law Section will make a determination on your request and notify you of its decision. If your request is approved, reimbursement will be provided upon completion of the written and oral presentations. Determinations as to whether a request is granted, and how many are granted, are within the sole discretion of the Council.

2002 Edward F. Langs Writing Award
ESSAY COMPETITION RULES

1. The award will be given to the student article, which in the opinion of the judges makes the most original and significant contribution to the knowledge and understanding of current computer law issues. The article should demonstrate original, creative and useful thought and insight into the law relating to computers.
2. The top three papers will receive awards of $500, $300 and $200 respectively (in US dollars)
3. All entries must be original and must not have been submitted to any other contest within the last 12 months.
4. All entries must include the submitter's name(s), current address, current telephone number and college or university attended.
5. All articles must be typed, double-spaced and submitted on letter-size (8½ by 11 inch) plain, white, bond paper (no onion skin).
6. Entries must be typed with margins of 10 and 70, respectively, along with top and bottom margins of no less than one inch each.
7. All entries must contain proper citations, including footnotes at the end of the entry.
8. Entry of at least 10 pages is preferred.
9. All rights to the entries shall become the property of the State Bar of Michigan.
10. The Computer Law Section reserves the right to make editorial changes.
11. The entry must be post-marked by June 30, 2002.
12. Entries are to be mailed to:
    David R. Syrowik, Chairman
    Computer Law Section Essay Competition
    Brooks & Kushman P.C.
    1000 Town Center, 22nd Floor
    Southfield, Michigan 48075

Computer Law Section
Michael Franck Building
State Bar of Michigan
306 Townsend Street
Lansing, Michigan 48933

Presorted
First Class Mail
U.S. Postage Paid
Lansing, MI 48933
Permit No. 191