Wisconsin Lawyer

Vol. 71, No. 12, December 1998

The Computerized Lawyer

Law Enforcement in Cyberspace: Search and Seizure of Computer Data

By Michael K. McChrystal,
William C. Gleisner III, & Michael J. Kuborn

How are computers and computer data viewed under the Fourth Amendment to the U.S. Constitution? The answer may both surprise and trouble you.

Have you ever considered what might become of a floppy disk containing sensitive information that you or a client throw away or lose? What about the hard drives in those computers you just replaced with new 450 megahertz systems? What if they fell into the hands of federal or state prosecutors? What about email or sensitive information you send to or receive from a client, even if it's encrypted? You may not have given this much thought, but the Department of Justice has. The DOJ's Federal Guidelines for Searching and Seizing Computers is available online, thanks to the Freedom of Information Act.[1]

Fourth Amendment standards

Fourth Amendment protections against unreasonable searches and seizures of an individual's personal possessions apply to agents of all levels of government - federal, state, and local[2] - whether the individual's activities are criminal or civil.[3] These protections are available only if a reasonable expectation of privacy is demonstrated by the individual with respect to those possessions. When a reasonable expectation of privacy is not demonstrated, our courts have

ruled that no improper "search" occurs.[4] Most courts, for example, have found that a person's garbage, once placed outside his or her immediate control, lacks the required privacy interest.[5] In fact, even documents cut into minute strips by a paper shredder involve no greater privacy interest than that afforded to the rest of the garbage with which they are disposed.[6]

A two-part test has been developed to determine whether a reasonable expectation of privacy exists. First, the individual by his or her conduct must have exhibited an actual (subjective) expectation of privacy. Secondly, that subjective expectation must be one that society is prepared to recognize as reasonable (when viewed objectively).[7] Even if there is a reasonable expectation of privacy, protections against unreasonable searches are by no means absolute. Once a reasonable expectation of privacy has been established, evidence sufficient to demonstrate probable cause that a crime has been, is being, or will be committed, will in most instances allow the issuance of a search warrant. Warrant requests to search files that contain privileged information generally are subject to the same standards.[8]

Search warrants are subject to attack, however, if they are overbroad in their language, or fail to specify with particularity the locations to be searched and the items to be seized. Historically, these concepts were developed with reference to tangible physical space and those items found residing there. Computer data doesn't fit the historical mold.

Computer data

One thing is certain: If someone surrenders physical control over computer equipment or data, he or she loses the expectation of privacy that is fundamental to protecting against governmental intrusion into the information that may reside there.[9] However, what if an individual attempts to delete files from a computer that is seized later pursuant to a valid search warrant? Those attempted deletions have not established a reasonable expectation of privacy for Fourth Amendment purposes.[10]

What if a law firm, or one of its clients, decides to surrender control of a computer to an outside consultant to perform maintenance or other service work? In the Seventh Circuit, the firm or the client proceeds at their considerable peril. In *United States v. Hall*[11] the defendant took his computer system to a repair shop for service. In the course of making repairs, a technician discovered image files that contained child pornography. The technician called a detective who called in the FBI, all unbeknownst to the defendant. Several interviews of the technician were conducted, and the FBI recruited the assistance of the computer shop to prolong repair on the defendant's computer while the FBI sought and obtained a search warrant. The court found no Fourth Amendment violation.

If surrendering a computer to an outside repair facility can compromise Fourth Amendment rights, what of the attorney-client privilege? Sending firm computers out for repair, and perhaps even using onsite consultants to service systems, could lead to many unfortunate consequences. The *Hall* decision needs to be considered in light of ABA Formal Ethics Opinion 95-398:

"A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information. Should a significant breach of confidentiality occur, the lawyer may be obligated to disclose it to the client."

When the Fourth Amendment is applied to computer data, three computer-related issues can

arise. The physical location of computer data can present difficult questions of jurisdiction and scope. Also, the scope of a search for computer data regularly requires a more expansive warrant than courts historically have tolerated. Finally, the form that the computer data takes may significantly affect the search.

Location

A search warrant that describes a particular file cabinet or set of such cabinets in a person's office rarely has given rise to overbreadth concerns. However, "because the architecture of cyberspace is dissimilar to most conventional notions of place, analogizing cyberspace to a place for Fourth Amendment [purposes] has serious limitations."[12] Data accessible by a particular computer system can reside in many different locations. Network systems almost always will store the actual data at a different site than where it was created or can be accessed. Any computer system with a modem attached exponentially increases possible storage locations. This not only greatly increases the opportunities for challenges to a search warrant, but can pose jurisdictional problems as well. If a person operates a fraudulent business enterprise, creating and maintaining all of his or her records on a computer system located in Milwaukee but stores that data on a server located in Illinois, can a Wisconsin court authorize its seizure from Milwaukee? When a "hacker" breaks into your client's computer system by using a series of different modem connections, each located in a different state, can local law enforcement ever hope to gain the evidence necessary for prosecution?

Scope of the search and seizure

A search warrant request for a particular manila folder could be challenged successfully if that warrant authorized the seizure of an entire room of file cabinets. On the other hand, locating a particular file on a computer system, even if the file name is known, regularly will require the seizure of large parts of the system, if not the entire system. This seeming inconsistency is a product of at least two characteristics of computer systems. First, the particular computer program that created the file and even the particular hardware being used helps define how access to the file is gained.[13] Second, unlike a filing cabinet where finding a particular manila folder will permit access to everything inside, computer information can be less tidy. An appellate brief that took days to produce will, despite the author's best efforts, reside in a multitude of different locations on a hard drive. Not only can those locations be lost or changed with a few keystrokes, but the brief can be saved in parts that entail a nearly infinite number of addresses or file names. Thus, a thorough government search of a client's computer system regularly will require law enforcement officers to seize all parts of the company's computer system, even if it seriously disrupts the company's business.

The wholesale removal of computer equipment undoubtedly can disable a business or professional practice and disrupt personal lives. However, until technology and law enforcement expertise make it possible to conduct a thorough search of a computer system onsite, wholesale seizures likely will be permitted.[14]

Form of computer data

Computers can make data either amazingly simple or amazingly difficult to access. At one end of the spectrum, encryption techniques, powered by computers capable of performing millions of operations in less time than it takes to yawn, have hampered many attempts to search and

seize computer data. At the other extreme, computer searches for all the documents your office created in a particular time period, a nearly impossible task when dealing with filing cabinets, can be performed in a matter of minutes. Since individual computer hardware components, as part of an overall system, are easily exchanged and modified by the user, data may exist simultaneously in a multitude of different forms, including CD-ROM, diskettes, one or more hard drives, several different tape backups, and in print. A commentator recently offered this analysis of the effects of encryption and password protection under the Fourth Amendment:

"Unlike a communication hidden by a password, an encrypted message can still be viewed, albeit in encoded form. For this reason, despite some commentators' assertions, encrypting one's communication is insufficient to establish a reasonable expectation of privacy. The encryption may obscure the meaning of a message but the encrypted message itself remains in plain view; thus, an officer's observation of that encrypted message is not a search and does not implicate the Fourth Amendment. Furthermore, the encoded message, once observed, may be decoded without implicating the Fourth Amendment, just as law enforcement agents may 'decode' communications that they overhear in other languages."[15]

The commentator also argues that "cyberspace communication should be protected with a password to establish a reasonable expectation of privacy. The password functions like a closed container or a seal on a letter; it hides from view the contents of the message. [L]aw enforcement agents should be required to obtain a warrant before trying to defeat a password just as they must obtain a warrant (absent some exigency) to open a closed container or a sealed package in the mail."[16]

With regard to email and other electronic communications, encryption and passwords will not necessarily provide protection from governmental access. A decision by the Court of Military Appeals suggests that an email message is like an unopened letter until the recipient retrieves it to his or her computer.[17] Once opened, the privacy of the email no longer is within the sender's control. Thus, the Fourth Amendment protects the electronic communication from interception, but the protection may be lost once the communication is complete.

Michael McChrystal, top, Marquette 1975, is a professor of law at the Marquette University Law School.

William Gleisner, middle, Marquette 1974, both a practicing attorney and computer consultant, maintains a law firm-based litigation support service bureau in Milwaukee.

Michael Kuborn, bottom, Marquette 1998, is with Olsen, Kloet, Gundersen & Conway, and is trained in computer recovery and computer search and seizure techniques. Products and services mentioned in this article should not be construed as an endorsement.

Conclusion

In terms of the Fourth Amendment, the steps one takes to prevent any actual government intrusion are not as important as the measures one takes to ensure that information is regarded, and treated consistently, as private. There are many ways to lose the protection of the Fourth Amendment for computer data. If you or your client surrender hardware or data to even the most trusted third parties, or are careless in your disposal of same, you run the considerable risk that a court might determine that the all-important reasonable expectation of privacy under the Fourth Amendment has been lost. In addition, information, even though encrypted, will be vulnerable if it is not protected from prying eyes by means of password

protection or some other design to restrict access to those clearly authorized. "A failed attempt at secrecy by reason of underestimation of police resourcefulness"[18]will be cold comfort to you or your clients if the government comes calling.

Endnotes

[1]To obtain a comprehensive guide to the state of Fourth Amendment law as it applies to computers, request the Federal Guidelines for Searching and Seizing Computers (1994) and its Supplement (October 1997) from the U.S. Department of Justice, Criminal Division, Computer Crime & Intellectual Property Section by mail or from its Web site.

[2]*See, New Jersey v. T.L.O.*, 469 U.S. 325 (1985).

[3] *See, e.g., Marshall v. Barlow's Inc.*, 436 U.S. 307 (1978); *Camara v. Municipal Court*, 387 U.S. 523 (1967).

[4] *See, United States v. Jacobsen*, 466 U.S. 109 (1984).

[5] *See, California v. Greenwood*, 486 U.S. 35 (1988); *but see contra, State v. Hempele,* 576 A.2d 793 (1990).

[6] *United States v. Scott,* 975 F.2d 927 (1st Cir. 1992).

[7] *See, Smith v. Maryland*, 442 U.S. 735 (1979).

[8]*See, Klitzman v. Krut,* 744 F.2d 955 (3rd Cir. 1984).

[9] *United States v. Redman,* 138 F.3d 1109, 1112 (7th Cir. 1998); *United States v. Scott,* 975 F.2d 927, 930 (1st Cir. 1992).

[10] *Pennsylvania v. Copenhefer,* 587 A.2d 1353, 1356 (Pa. 1991).

[11] 142 F.3d 988 (7th Cir. 1998).

[12] *Note, Keeping Secrets in Cyberspace, Establishing Fourth Amendment Protection for Internet Communication,* 110 Harv. L. Rev. 1591, 1599-1601 (1997).

[13] This explains some problems that occur in offices using more than one system or for people who do work at home on a system different from the one at work.

[14] *United States v. Hunter,* 13 F. Supp. 2d 574, 583 (D. Vt. 1998).

[15]*Note 12, supra,* at 1604.

[16] *Id.*

[17] *United States v. Maxwell,* 45 M.J. 406, 418 (C.M.A. 1996).

[18] *United States v. Scott, supra,* note 9 at 930.

Wisconsin Lawyer Main

WisBar Main

Problems? Suggestions? Feedback? Email Wisconsin Lawyer

Disclaimer of Liability

Statements or expressions of opinion in the *Wisconsin Lawyer* are those of the authors and not necessarily those of the State Bar or editors. Due to the rapidly changing nature of the law, information contained in this publication may become outdated. As a result, lawyers using this material must research original sources of authority. In no event will the authors, the editors, the reviewers or the publisher be liable for any damages resulting from the use of this material.

The publication of any advertisement is not to be construed as an endorsement of the product or service offered unless the ad specifically states that there is such an endorsement or approval.

The State Bar of Wisconsin presents the information on this web site as a service to our members and other Internet users. While the information on this site is about legal issues, it is not legal advice. Moreover, due to the rapidly changing nature of the law and our reliance upon information provided by outside sources, we make no warranty or guarantee concerning the accuracy or reliability of the content at this site or at other sites to which we link.

Terms and Conditions of Use