Global Information Assurance Certification Paper

GATHERING ELECTRONIC EVIDENCE UNDER THE GUIDELINES OF THE FOURTH AMENDMENT WITHOUT SEARCH WARRANTS

Christopher M. Logan

SANS Security Essentials
GSEC Certification
Version 1.4c

March 18, 2005

Table of Contents

ABSTRACT

Digital technology has changed the way we conduct our everyday lives. Through these bright new and advanced innovations we have grown in more ways than was conceivable ten years ago. Not only have we, the public, been able to grow with this technological boom but so have common criminals. The intention of this practical assignment is to provide insight and allow the general Information Technology practitioner to better understand how electronic evidence is gathered without using search warrants. I will also discuss how the Fourth Amendment characterizes these searches while defining the various types of searches which fall under the exceptions of warrant requirement rules for gathering electronic evidence.

INTRODUCTION

Fred Galves, a law professor at the University of Pacific states that new and advanced technology is allowing criminals direct access to our lives, as no proverbial right or wrong side of the tracks exists to divide the safe from the unsafe in cyberspace.[1] The scariest thought surrounding this statement is it is absolutely true. Think about this, if you were to go to a mall and a criminal wanted to rob you he would have to physically confront you while demanding your wallet. In today's electronic society all the criminal has to do is be armed with a laptop and an internet connection. While gathering information about you he can wipe out your bank account by simply pushing a few buttons.

Galves continued by stating that this technology has introduced crime as a career for many who previously may have found committing crime the old-fashioned way, such as robbing or kidnapping, involved too much work or risk.[2] With the extent of ease technology has made on everyday life it has also made the art of committing crime that much easier.

Computers and digital media seem to be increasingly involved in unlawful activities. The computer may act as contraband, fruits of the crime, a tool of the offense, or a storage container holding specific evidence. Any investigation of criminal activity might produce some form of electronic evidence. It is imperative law enforcement officers recognize, protect, search, and seize computers and digital storage devices in accordance with applicable statutes, policies, and best practices/guidelines. People who deal with any form of Information Technology on a daily basis should also share this sound understanding.

THE FOURTH AMENDMENT

The law governing electronic evidence in criminal investigation has two primary sources: the Fourth Amendment to the U.S. Constitution, and the statutory privacy laws codified at 18 U.S.C. 2510-22, 18 U.S.C. 2701-12, and 18 U.S.C. 3121-27.[3] The Department of Justice manual," Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Cases,"[4] identifies the

---

[1] Galves, Fred and Christine Galves, "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probable Value at Trial," Criminal Justice Magazine Vol. 19, No. 1. Spring 2004. <http://www.abanet.org/crimjust/cjmag/19-1/electronic.html>

[2] See Fred Galves article.

[3] "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Cases." July, 2002. Computer Crimes and Intellectual Property Section, Criminal Division, United States Department of Justice. <http://www.cybercrime.gov/s&smanual2002.htm>

[4] "Searching and Seizing" Introduction, viii.

constitutional and statutory issues overlap in many cases. The Fourth Amendment is the set standard for search and seizure while statutory issues commonly involve computer networks and internet service providers.

The Fourth Amendment of the U.S. Constitution limits the ability of government agents to search for any type of evidence without a warrant. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search 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.[5]

According to the Supreme Court, a search can be warrantless if it satisfies two conditions. First, in the case Illinois v. Andreas, 463 U.S. 765 (1983), the government's conduct cannot violate the person's reasonable expectation of privacy. If there is none, then it is not a Fourth Amendment search and requires no warrant.[6] Second, in the case Illinois v. Rodrigues, 497 U.S. 177 (1990), a warrantless search that violates a person's reasonable expectation of privacy will be constitutional if it falls within an established exception to the warrant requirement.[7] This is the measure all investigators must meet regarding search requirements for a warrant, based on the above criteria. Later on in this paper I will explain some circumstances involving the established exceptions to the warrant requirement.

GENERAL PRINCIPLES

We have already concluded a search is only constitutional if it does not violate a person's legitimate expectation of privacy. An older case which identified this expectation is Katz v. United States, 389 U.S. 347 (1967).[8] This case in particular answered two questions which help us better understand the level of expected privacy. First, does the individual's conduct reflect an actual expectation of privacy? Second, is the individual's expected level of privacy one that society will recognize?

This problem can be tough to identify and has been split on many occasions. So where is the line drawn when determining your constitutional rights? One case reflecting this line is O'Connor v. Ortega, 480 U.S. 709 (1987).[9] In this

[5] Samaha, Joel. "Criminal Procedure" Wadsworth/Thompson Learning, California. 2002
[6] Illinois v. Andreas, 463 U.S. 765 (1983)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=463&page=765>
[7] Illinois v. Rodrigues, 497 U.S. 177 (1990)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=497&page=177>
[8] Katz v. United States, 389 U.S. 347 (1967)
< http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=389+&page=347>
[9] O'Connor v. Ortega, 480 U.S. 709 (1987)
< http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=480&page=709>

case, a practicing doctor was suspected of sexual misconduct and harassment of a trainee. A supervisor searched his office to include his personal belongings while he was on vacation. These personal belongings included his computer, a file cabinet, his desk, and other items. This was deemed inappropriate by the Supreme Court because the Fourth Amendment allows an expectation of privacy in one's place of work. This is in fact based upon societal expectations which are deeply rooted in the history of the amendment. However, the operational realities of the workplace may make some public employees' expectations of privacy unreasonable when an intrusion is conducted by a supervisor rather than a law enforcement official.

REASONABLE EXPECTATION OF PRIVACY WITH COMPUTERS AS STORAGE DEVICES

In determining whether or not an individual has an expectation to privacy when dealing with information stored on a computer it is always useful to treat that computer as a closed container. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored on a computer without obtaining a warrant first.

This concept was first noted in the case United States v. Ross, 456 U.S. 798 (1982). This case determined people can expect reasonable amounts of privacy in the contents of a closed container and generally retain this same amount of privacy with data stored on an electronic device. The court ruled people do in fact have a reasonable amount of privacy with storage devices such as computers when they are under the individual's personal control.

Although individuals generally retain a reasonable expectation of privacy in computers under their control, special circumstances may eliminate that expectation. For example, an individual will not retain a reasonable expectation of privacy in information from a computer when the person has made it openly available. In United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), agents looking over the defendant's shoulder read the defendant's password from the screen as the defendant typed this password onto a handheld computer. The court found no Fourth Amendment violation in obtaining the password because the defendant did not demonstrate an expectation of privacy "in the display that appeared on the screen." Nor will individuals generally enjoy a reasonable expectation of privacy in the contents of computers they have stolen.[10]

REASONABLE EXPECTATION OF PRIVACY AND THIRD PARTY POSSESSION

Individuals generally retain a reasonable expectation of privacy in stored electronic information under their control. This expectation is diminished under the Fourth Amendment when relinquishing that control to third parties. Examples of this include when an individual offers a container of electronic

[10] Peikari, Cyrus and Seth Fogie. "Legal Controversies Part 3: Search and Seizure." < http://www.informit.com/guides/content.asp?g=security&seqNum=114&rl=1>

information (items consisting of hard drives, or any other type of digital storage media) to a third party such as a repair shop. There can even be a diminished right to privacy when shipping electronic storage containers via mail to another party. A second alternative is the transmission of digital data to a third party over either an internal network or the internet.

To analyze third party possession concerns, two types of possession must be established. The first type is possession by some form of carrier during the course of transmission to the intended recipient. This might be traversal of the network infrastructure and it might be the use of a commercial courier system such as the US Mail. The second type is the subsequent possession of the digital information by the intended recipient. Hiring a commercial company to carry a package to a colleague, there remains a reasonable expectation of privacy for the contents of that package during transit. However, when the package arrives at its destination, the expectation of privacy can differ significantly based on the circumstances. The key understanding here is that in the course of transmission, contents are generally covered by Fourth Amendment protections.

In the case Berger v. New York, 388 U.S. 41 (1967), the government had intercepted wire transmissions from the defendant without obtaining a warrant.[11] The ruling was this was in fact a breach of the defendant's Fourth Amendment rights because the information was captured in transit through a third party provider. At the time, boundaries for these types of cases where very questionable which enabled Congress to pass Title III of the Omnibus Crime Control and Safe Streets Act of 1968. This act provides a comprehensive statutory framework that regulates real time monitoring of wire and electronic communications.[12]

Another important facet of privacy identified through Supreme Court cases is that individuals cannot expect to retain control over information revealed to government–regulated agencies. This is true even if the sender maintains a subjective expectation that the third party will keep all of the information provided confidential. This was especially evident in the case United States v. Miller, 425 U.S. 435 (1975).[13] The court held the Fourth Amendment does not protect bank account information which account holders divulge to the bank. By simply placing that information under the control of a financial institution, the account holder assumes the risk that the information will be conveyed to the government or one of its agents. This was also the case in Couch v. United States, 409 U.S. 322 (1973), where the government utilized its rights to subpoena private information from an accountant (a regulated entity) to conduct an investigation.[14]

---

[11] Berger v. New York, 388 U.S. 41 (1967) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=388&page=41>

[12] "Searching and Seizing Manual" pg 5.

[13] United States v. Miller, 425 U.S. 435 (1975) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=425&page=435>

The key here is that persons or organizations whose duties are regulated by the government have an obligation to report evidence of illegal activity to law enforcement. This obligation on the part of the third party overcomes the expectation of privacy on the part of the owner of the data.

Because digital storage is considered a closed container for privacy purpose, it is important to remember that the data itself is simply considered information. When information is being transmitted in a form that is not considered a closed container such as over an intranet or network, the expectation of privacy can be diminished in certain instances. The cases listed above suggest that any individual sending data over any type of communication network may in fact lose his or her Fourth Amendment protection for the data, either in transmission or once it reaches the intended recipient. Even though this is the case, the absence of constitutional protection does not necessarily mean that the government has access to that data without a warrant or court order. Statutory protections do exist which generally protect the privacy of electronic communications which are stored remotely with a service provider. These statutory regulations may also protect the privacy of Internet users where the Fourth Amendment may not apply.[15]

PRIVATE SEARCHES

The Fourth Amendment does not apply to searches conducted by private parties who are not acting as agents of the government. An example of this is United States v. Hall, 142 F.3d 988 (7th Cir. 1998). In this case, the defendant had taken his computer to a private repair shop for evaluation. During that evaluation, the computer specialist observed some files which had very similar characteristics to what appeared to be child pornography. Upon accessing the files, the computer technician confirmed the files were in fact child pornography. He then notified the state police which led to the granting of a warrant, the defendant's arrest and conviction for child pornography offenses.[16]

On future appeal, the court held the warrantless search by the repairman did not violate any form of the Fourth Amendment because the search was conducted on his own. Generally, there is no violation of the Fourth Amendment when a private individual, acting on his own accord, conducts a search and makes the subsequent results available to law enforcement. It is easy to understand the defendant surrendered his rights when he delivered the computer and its contents to a third party.

THE USE OF TECHNOLOGY TO GATHER INFORMATION

The government will in fact violate the Fourth Amendment if they use new technology to gain information in searches as we can see in the case Kyllo v.

---

[14] Couch v. United States, 409 U.S. 322 (1973) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=409&page=322>

[15] "Searching and Seizing Manual" pg 6

[16] "Searching and Seizing Manual" pg 7

United States, 533 U.S. 27 (2001). The Supreme Court in that case held the government's use of a thermal imager to reveal substantial amounts of heat from the defendant's home was in fact a violation of the Fourth Amendment. In particular, law enforcement agents require a warrant to use technology not generally available for public use. This technology would be used to explore details of homes or other closed containers that would previously have been unknown without a physical intrusion. The surveillance is in fact a search and is unreasonable without obtaining a warrant. For all the same reasons stated above, the government is also not allowed to use technology when conducting searches of computers or networks. If the tools they are using to obtain information are not being used by the general public then they must employ the rules set forth in the Kyllo case and acquire a search warrant.[17]

EXCEPTIONS TO THE WARRANT REQUIREMENT

By general rule and if time and circumstances permit, the best route in an investigation is to always obtain a warrant. This method allows for a proper legal assessment of the given situation. However if the investigating party decides to make a warrantless search in a case involving a computer, it must comply within several different guidelines.

CONSENT

The most obvious of these exceptions is consent. There are two attributes to consent searches. They are the question of voluntary consent, and the authority to provide consent for a given search. An investigator may search without a warrant or even probable cause if the person with authority over the electronic information voluntarily consents to the search. For the most part, the voluntary nature of the consent can be resolved with the use of consent forms. Of course the issue raised out of all consent searches is the governments burden of proving the consent was voluntary.

Third party consent for a warrantless search can become tricky. This issue has seen an overwhelming debate in cases such as the United States v. Matlock, 415 U.S. 164 (1974).[18] This case involves third party consent and it was deemed appropriate to conduct a search with the permission of the person who also has common authority over the property. This predicament is also prevalent in computer cases because under normal circumstances it is possible to have more than one owner of a personal computer (for example, husband and wife).

EXIGENT CIRCUMSTANCES

The next exception to obtaining a warrant would be in exigent circumstances.

[17] Kyllo v. United States, 533 U.S. 27 (2001) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=533&page=27>

[18] United States v. Matlock, 415 U.S. 164 (1974) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=415&page=164>

This exception is valid if it appears a search or seizure was necessary to protect law enforcement or the community, prevention of destruction of relevant evidence, the escape of a suspect, or any other consequence hindering law enforcement efforts. This is defined in the case United States v. McConney, 728 F.2d 1195, 1199 (9thCir,), certiorari denied, 469 U.S. 824 (1984).[19]

Exigent circumstances are very common when dealing with electronic evidence because data can be destroyed very easily. Data is not strictly vulnerable to just computer commands. Weather, such as humidity and extreme temperatures, physical destruction, and even magnetic fields can destroy electronic evidence. An example of an exigent circumstance can be found in United Stated v. David, 756 F.Supp, 1385 (D.Nev. 1991). In this case the law enforcement officer had witnessed the defendant deleting files on his personal computer and seized the computer immediately to protect the evidence. The defendant's actions had created an exigent situation.[20]

Most importantly any exigent circumstance does not allow a law enforcement officer to search or seize beyond what is deemed necessary to prevent the destruction of evidence. It is understandable they need to take certain steps to prevent the loss of data but it does not authorize them to take further action without a warrant.

PLAIN VIEW

Evidence may also be seized through exception to the warrant requirement through the plain view doctrine. To rely on this doctrine the investigator must be in a lawful position to observe and access the evidence and it must display some sort of incriminating characteristics. In the case Horton v. California, 496 U.S. 128 (1990), the warrant issued did not explicitly identify the items that were seized because they were in plain view. The Supreme Court has ruled this does not violate any Fourth Amendment rights because of the plain view doctrine.[21]

The concern with the plain view doctrine is whether data on computer hard drives should be treated as closed containers? The courts have generally split decisions regarding this topic. They simply state accessing the information contained on the device is just like opening a closed container. According to United States v. Ross, 456 U.S. 798 (1982), individuals generally retain a reasonable expectation of privacy when dealing with the contents of closed containers.[22] With this stated, accessing information stored on a computer will implicate the owners reasonable expectations of privacy of the data stored within. This conclusion was evident in the case United States v. Barth, 26 F.

---

[19] "Legal Definition of Exigent Circumstances" < http://www.lectlaw.com/def/e063.htm>

[20] "Search and Seizure Manual" pg 19

[21] Horton v. California, 496 U.S. 128 (1990) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=496&page=128>

[22] United States v. Ross, 456 U.S. 798 (1982) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=456&page=798>

Supp. 2d 929, 936-37 (W.D. Tex. 1998).[23]

SEARCHES INCIDENT TO A LAWFUL ARREST

The next exception to the warrant rule is the search investigators may conduct after lawfully arresting an individual. According to the rule they can perform a full search of the person and a limited search of the surroundings. This becomes problematic when the person has an electronic storage device such as a pager, personal digital assistant, cell phone, or laptop computer. In United States v. Reyes, 992 F. Supp. 818, 833 (S.D.N.Y. 1996), the court determined an officer who accessed an electronic pager carried by the arrested person was a valid search incident to a lawful arrest.[24] One question arises from this: how much of a search is permitted without a warrant since any search incident to an arrest must be reasonable? This case also documents what can be expected in a situation dealing with any electronic storage device. Whenever in doubt there should always be a warrant obtained in situations dealing with electronic evidence.

INVENTORY SEARCHES

Due to the nature of seized evidence, inventory searches are very common for law officers. These inventory searches are considered reasonable so they fall under the exception to the warrant requirement. This requires two conditions, the search must be legitimate and for non-investigative purposes to protect the property while in custody while not intruding on the individuals Fourth Amendment rights, and the search must follow specific procedure or protocol. This scenario is demonstrated in Illinois v. Lafayette, 462 U.S. 640 (1983). After the arrested man was taken into custody an inventory search was done on his belongings leading to the discovery of drugs which was then used against him.[25] It is not evident an inventory search exception to the warrant requirement would support a search through seized computer files or other electronic devices.

BORDER SEARCHES

The final exception to warrant requirement is for border searches. Border searches have been enabled by the Supreme Court to allow the government the ability to monitor contraband and other property entering or exiting the United States illegally. According to United States v. Montoya De Hernandez, 473 U.S. 531 (1985), routine searches at the border or its functional equivalent do not require a warrant, probable cause, or even reasonable suspicion the search may uncover contraband or evidence.[26] The sole purpose for these non-warrant searches is the best interest of the United States and its citizens.

---

[23] "Search and Seizure Manual," Pg 2

[24] See Fred Galves article.

[25] Illinois v. Lafayette, 462 U.S. 640 (1983)
< http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=462&page=640>

[26] United States v. Montoya De Hernandez, 473 U.S. 531 (1985)
< http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=473&page=531>

CONCLUSION

This paper has just touched a small portion of the legal aspect of how electronic evidence is gathered without the use of a search warrant. Many other topics could be discussed when dealing with electronic evidence such as special case scenarios, and further Fourth Amendment issues when responding to the reasonable expectation of privacy regarding computers and electronic storage devices. This subject has been and will continue to gain attention throughout the legal world and will eventually be documented very thoroughly.

Albert Einstein once said that technological progress is like an axe in the hands of a pathological criminal.[27] He appears to be correct stating this because technology in the twenty-first century has not only enhanced our lives, but has also become a dangerous tool for criminals. Within the Information Technology arena, practitioners must understand how legal requirements relate to the industry. It is incumbent on us as a community to assist law enforcement in any manner in protecting our networks, assets, and personal lives.

[27] Einstein, Albert. Quote < http://www.quotationspage.com/quote/20767.html>

REFERENCES

Berger v. New York, 388 U.S. 41 (1967)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=388&page=41>

Couch v. United States, 409 U.S. 322 (1973)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=409&page=322>

Einstein, Albert. Quote < http://www.quotationspage.com/quote/20767.html>

Galves, Fred and Christine Galves, "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probable Value at Trial," Criminal Justice Magazine Vol. 19, No. 1. Spring 2004.
<http://www.abanet.org/crimjust/cjmag/19-1/electronic.html>

Horton v. California, 496 U.S. 128 (1990)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=496&page=128>

Illinois v. Andreas, 463 U.S. 765 (1983)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=463&page=765>

Illinois v. Lafayette, 462 U.S. 640 (1983)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=462&page=640>

Illinois v. Rodrigues, 497 U.S. 177 (1990)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=497&page=177>

Katz v. United States, 389 U.S. 347 (1967)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=389+&page=347>

Kyllo v. United States, 533 U.S. 27 (2001)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=533&page=27>

"Legal Definition of Exigent Circumstances"
<http://www.lectlaw.com/def/e063.htm>

O'Connor v. Ortega, 480 U.S. 709 (1987)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=480&page=709>

Peikari, Cyrus and Seth Fogie. "Legal Controversies Part 3: Search and Seizure."
<http://www.informit.com/guides/content.asp?g=security&seqNum=114&rl=1>

Samaha, Joel. "Criminal Procedure" Wadsworth/Thompson Learning, California. 2002

"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Cases." July, 2002. Computer Crimes and Intellectual Property Section, Criminal Division, United States Department of Justice.
<http://www.cybercrime.gov/s&smanual2002.htm>

United States v. Matlock, 415 U.S. 164 (1974)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=415&page=164>

United States v. Miller, 425 U.S. 435 (1975)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=425&page=435>

United States v. Montoya De Hernandez, 473 U.S. 531 (1985)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=473&page=531>

United States v. Ross, 456 U.S. 798 (1982)
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=456&page=798>