3-1-2005

Computer Forensics Search and Seizure: Challenges in Academe

Michael Whitman
mwhitman@kennesaw.edu

COMPUTER FORENSICS SEARCH AND SEIZURE: CHALLENGES IN THE ACADEME

Michael E. Whitman
Kennesaw State University
mwhitman@kennesaw.edu

Abstract

As faculty members teach and conduct research within their institutions, they should be secure in the knowledge that the intellectual property they create is free from concern of loss of confidentiality, and that the computer systems entrusted to them to perform this work will not be seized and scrutinized without formal process and legal procedure. However, unless the institution and its constituent groups have co-developed relevant, salient and legally compliant policy, the search and seizure of computer-based information, could turn into a political nightmare. This paper examines the laws relevant to computer search and seizure as they apply in the academe.

Keywords: Computer Forensics, Fourth Amendment, Search and Seizure, Academic Freedom, Intellectual Property

Introduction

The field of Computer Forensics is rapidly evolving from its origins as an offshoot of criminal justice forensic studies and becoming a more complete sub-topic within the information security discipline. Organizations are increasingly able to monitor workplace behavior to determine if criminal activities or work-related misconduct has occurred either in real-time using network or client-based tools, or after the fact using the tools of computer forensic analysis. In the face of ever-advancing technologies, the trained forensic analyst is capable of performing the mission to acquire, authenticate, analyze and report the presence or absence of evidentiary material stored on computer media.

The most significant questions facing computer forensics aren't technological; but are rather legal, ethical and managerial. The challenge is not whether or not the investigator can seize and examine computer media, but rather should they? The decision to search for and seize potential evidentiary material has proven to be a legal quagmire. While there are some straightforward guidelines to aid those operating within the private sector, it is not as straightforward for organizations in the public sector, especially academic organizations. Through this work the author examines the factors that should inform and influence decisions to search for and seize information found on computer systems in the public sector. It presents information discovered in this topic area and makes recommendations for academic institutions, and the faculty staff and students who populate these institutions as to the proper approach to balance the privacy needs of the university's constituents with the information security and legal needs of the institution.

The Fourth Amendment and Workplace Searches

At the heart of the problem of institutional search and seizure of computing equipment is the consideration of personal privacy as alluded to in the Fourth Amendment of the US Constitution, 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 (US Constitution, 1787).

The Fourth Amendment establishes that the people have a right against searches of our person and property unless duly authorized by appropriate agencies of government. This "expectation of privacy" has been stretched by case law to include the workplace. It may seem contradictory that a worker has an expectation of privacy in the workplace, but the courts have determined that this is sometimes so. In Warden v. Hayden the Supreme Court held that the Fourth Amendment principally protected privacy rights, not property rights (Hayden, 1967).

Warrantless Searches and the Public Sector

In O'Connor v. Ortega (1987) the Supreme Court delineated the workplace into two sectors, public and private. As established in O'Conner and as illustrated in the Department of Justice's Manual for Computer Search & Seizure: "In public (i.e., government) workplaces, officers cannot rely on an employer's consent, but can conduct searches if written employment policies or office practices establish that the government employees targeted by the search cannot reasonably expect privacy in their workspace. Further, government employers and supervisors can conduct reasonable work-related searches of employee workspaces without a warrant even if the searches violate employees' reasonable expectation of privacy" (DoJ, 2002).

This clarification establishes a clear precedent for the public sector employer to conduct work-related searches. The employer or supervisor has the right to search a worker's area under the following conditions; 1) if the organization has established policy permitting such searches by employers, supervisors, co-worker or even the public, 2) in order to obtain work-related material such as reports of files needed to support the ongoing function of the organization, and 3) to investigate work-related misconduct. While an employer or supervisor doesn't need a warrant under these guidelines, they do need the organizational equivalent of probable cause; that is the search must be "justified at its inception and permissible in its scope" (DoJ, 2002). The former requires that there has to be a reasonable expectation that the search will provide evidence of work-related misconduct, or is part of a normal search – i.e. not fishing for evidence. This does allow the possibility that the employer or supervisor to use anything found when searching for something else. Permissible in its scope means that the search was a reasonable search and did not exceed the supervisor's or employer's scope of authority. This means the employer cannot look outside areas that would be part of a normal search, such as the personal belongings of an employee. This probable cause may be challenged if the employee chooses to contest the search, whether or not evidentiary material was found. If the employer or supervisor cannot produce some fact or corroborating evidence that suggested work-related misconduct, the search can be declared unconstitutional, any evidentiary material found during the search ruled inadmissible, and damages awarded the employee. Simply finding evidence of misconduct does not justify the search (US v. Hagarty, 1968).

The Expectation of Privacy

As the courts ruled in Katz v. United States (1967), "A search is constitutional if 1) the individual's conduct reflects 'an actual (subjective) expectation of privacy,' and 2) whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as 'reasonable' " (DoJ, 2002). In both the public sector, privacy essentially boils down to the level of expectation provided to the employee by policy. When the organization has clear policy stating that employees have no expectation of privacy, then warrantless searches can occur almost at will. However, simply having a policy permitting employers or law enforcement to search an employee's office without a warrant is not enough (Whitman & Mattord, 2005). Factors mitigating the expectation of privacy include the number of individuals with access to the space, the presence or absence of doors and locks, and indicators of the presence or absence of privacy in the workplace, as in written policies, posted notices, and electronic banners.

In general, government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers can have no reasonable expectation of privacy in the information stored there (See US v. Simmons, 2000)… Other courts have agreed with the approach articulated in Simons and have held that banners and policies generally eliminate a reasonable expectation of privacy in contents stored in a government employee's network account. (See US v. Angevine, 2002) (DoJ, 2002). Note that the simple presence of a warning, whether warning banner or employee handbook or manual may not be adequate (See US v. Angevine, 2002). In the absence of policy or warning banners, courts will almost assuredly infer an expectation of privacy in the use of a computer (See US v. Slanina, 2002). The challenge comes in the application of Fourth Amendment protection to computer media and the electronic information contained within. "To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation" (DoJ, 2002).

Exceptions to the Fourth Amendment

There are a number of exceptions to the requirement for warrants specified by the Fourth Amendment, as the courts have continually struggled with balancing reasonable expectations of privacy by the individual with the needs of law enforcement and organizations in conducting searches. With rapidly changing information technology how these exceptions are handled will be an ongoing challenge for the courts, organization and individuals. These exceptions include 1) Consent, 2) Plain View, 3) Exigent Circumstances, 4) Search Incident to a Lawful Arrest, 5) Inventory Searches, 6) Border Searches and 7) International Issues. The two most relevant exceptions are discussed here.

Consent Searches

If the individual or "person with authority" consents to the search, then no warrant is needed. The challenge is whether the consent is implicit or explicit, or whether it was voluntarily given. (See Schneckloth v. Bustamonte, 1973 & US v. Milian-Rodriguez, 1985). Fortunately for the individual, in criminal matters, the burden of proof is the governments. The problem arises under two issues: The first is the scope of consent – e.g. if an individual consents to the search of part of a system, does this infer consent to search the entire system? Second, who is authorized to provide this consent? Can family, friends, or roommates provide this consent? With regard to who can provide consent, if the technology is used or owned by more than one individual, any one of those individuals can consent to the search. As such there is no reasonable expectation of privacy (US v. Matlock, 1974).

Plain View Doctrine

An item is in plain view if it is readily observable by the investigator without manipulation of the environment in which the information resides (See Horton v. California, 1990). This also means that if an investigator is conducting a lawful search of a computer hard drive, and discovers evidence of another crime, the supplemental evidence is considered in plain view. However, if the investigator is authorized to search specific folders, and opens folders outside of the authorized search area, the discovered information may not be considered "in plain view" (See US v. Maxwell, 1996).

Complications Associated with Other Laws and Policy

It would appear from the discussion above that public academic institutions' employees would only enjoy Fourth Amendment protection to the extent provided to all public-sector employees. When just considering the Fourth Amendment, this may be the case. This would indicate that law enforcement needs a warrant, while the employer or employer's representative (e.g. department chair or dean) need only probable cause associated with work misconduct or suspicion of criminal conduct. However, there is another issue that complicates the Fourth Amendment interpretation. As stated in the DOJ search and seizure manual:

In many cases, workplace searches will implicate federal privacy statutes in addition to the Fourth Amendment. For example, efforts to obtain an employee's files and e-mail from the employer's network server raise issues under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712, and workplace monitoring of an employee's Internet use implicates Title III, 18 U.S.C. §§2510-2522 (DoJ, 2002).

One such statute is the 1976 Copyright Act (Title 17, U.S. Code) which extends protection to the owners of intellectual property. While this act in and of itself does not prevent an institution from seizing and searching computer systems in the public sector, its use in conjunction with organizational policy may. For example, if an employee at a University creates intellectual property and University policy indicates the individual owns the intellectual property and is entitled to 100 percent of any royalties derived from that intellectual property, then using this policy, it is a logical assumption that works leading to the development of intellectual property, resulting from the development of intellectual property and works in progress are all the personal property of the individual. When the University permits the individual to store their information (personal property) on equipment issued for their personal use, the University has given up the right to search and seize that property at will. There is a special case in the creation of intellectual property, which falls under the concept of work-for-hire - a situation where an employee creates intellectual property at the behest or requirement of an employer. In this case the employer is considered to be the author and thus the owner of the intellectual property (US Copyright Office, n.d.).

Special Cases in the Public Sector: The Academe

Faculty

Whereas faculty members in public institutions typically enjoy the most protection under the Fourth Amendment et al., that hasn't stopped some institutions from grabbing their machines for search (see for example McCaughey, 2003). Once the organization has the data, there is little recourse outside of civil litigation. The American Association of University professors (AAUP) can censure the institution for failure to sponsor an environment of academic freedom, but unless personal information is taken, there is little means of restitution. This is not to condone these heavy-handed institutional tactics, but is meant to warn the faculty of a worst-case scenario. Before entrusting critical research and teaching data to institutional systems, review the policies outlining the organization's intent to search and seize information systems and faculty data. If such policies do not exist, document the fact. Look for policies outlining clear and responsible use of the systems, on electronic monitoring, and on ownership of intellectual property for related statements. The most responsible method of ensuring that only warranted searches will access the faculty member's data, is to purchase your own external media storage

device, and store all personal data on it. Clearly label it as personal property and ensure the department chair, or other immediate supervisor is aware of the installation of personally owned technology on institutional systems. Use password protection or even encryption to protect the information. Any action taken by the institution to search and seize this device can be fought in criminal court quickly and effectively.

Staff

While Fourth Amendment protection applies equally to all public institution employees, there are often fewer chances that large numbers of staff members will be involved in the creation of intellectual property, and even slimmer chance that they will enjoy the protection of intellectual property. The harsh reality is that support staff more closely resemble private sector employee in this regard. The best advice for staff is don't put personal information or anything you don't want the University to see on organizational equipment.

Students

While the laws regulating the search of Faculty and Staff offices and equipment, the relationship between the institution and the student is a different matter. In 1985, the United States Supreme Court ruled in New Jersey v. T.L.O. (1985) that public school officials represent a special case – somewhere between the private citizen who searches without a warrant and a law enforcement official required to present probable cause in order to obtain a search warrant (DoJ, 2002). Student can consent to search if the area to be searched is under the ownership or control of the student. This extends to the student's property and any storage facility issued to the student for their exclusive use (as in a locker or dorm room), as long as there is an expectation of privacy (i.e. lockable facility).

The Institution

In order to ensure the most open, cooperative, and conducive working relationship between employees and the institutions, institutions should clearly outline policies developed in coordination with faculty and staff, carefully outlining the extent to which the institution can and should search institutional equipment. There are valid reasons for institutional representative to seize and search equipment. What should not occur are questionable searches which infringe upon the employees ability to conduct their work. If the institution desires to prevent the viewing and storage of objectionable material on organizational equipment, there must be methods to allow the continuation of legitimate, open, and fruitful research and instruction. While the institution does not have to allow uncontrolled abuse of privilege, it should seek to comply with the tenets of academic freedom, as described in the section below.

Academic Freedom

Notice the discussion thus far has avoided discussion of academic freedom. Academic freedom is defined as "the freedom of teachers and students to teach, study, and pursue knowledge and research without unreasonable interference or restriction from law, institutional regulations, or public pressure. Its basic elements include the freedom of teachers to inquire into any subject that evokes their intellectual concern; to present their findings to their students…" (Academic Freedom, n.d.). There is a difference between being permitted to conduct research and present one's findings, and being protected from its seizure. While there could be an overlap between the two, unless the individual intellectual property owner could prove the institution seized his or her information as a political interference, to censure or suppress the findings, then there is little protection to be found here. In addition, academic freedom is not based on law, but on tradition, which means the institution may find itself on the wrong side of the ACLU, the AAUP, or a number of other organizations threatening civil litigation, but not criminal.

CONCLUSION

The issues associated with the search and seizure of computer information in the academe are not always straightforward. This complexity is represented in the Fourth Amendment, the case law regarding searches and seizures, laws regarding intellectual property, organizational policies, and the professional courtesies associated with Academic Freedom. Academic organizations would be well served if the institution's administration and representatives of faculty, staff and students, along with the IT department, meet to create policy on the search and seizure of computer data within the institution. The clear definition of expectations for the privacy, of personal and intellectual property and the institutions expectations of individual performance with regard to the use of institutional equipment will go a long way to avoid many of these potentially litigious situations.

REFERENCES

Academic Freedom. (n.d.) Encyclopedia Britannica Online. Retrieved October 15, 2005 from http://www.britannica.com/eb/article?tocId=9003450&query=academic%20freedom.

DoJ (2002) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Retrieved September 10, 2004 from http://www.cybercrime.gov/searching.html.

Horton v. California. (1990) 496 U.S. 128.

Katz v. United States. (1967) 389 U.S. 347, 362.

McCaughey, M. (2003) Windows Without Curtains - Computer Privacy and Academic Freedom. Retrieved October 10, 2004 from http://www.aaup.org/publications/Academe/2003/03so/03somcca.htm.

New Jersey v. T.L.O. (1985) 469 U.S. 325.

O'Connor v. Ortega. (1987) 480 U.S. 709.

Robbins, J.(n.d.) Federal Guidelines for Searching and Seizing Computers. Retrieved October 15, 2004 from http://knock-knock.com/federal_guidelines.htm.

Schneckloth v. Bustamonte. (1973) 412 U.S. 218, 219.

U.S. Constitution. (1787) Fourth Amendment. September 17. Retrieved October 10, 2004 from http://caselaw.lp.findlaw.com/data/constitution/amendments.html.

U.S. Copyright Office. (n.d.) What is Copyright? Retrieved October 12, 204 from http://www.copyright.gov/circs/circ1.html#wci.

United States v. Angevine. (2002) 281 F.3d 1130, 1134-35 (10th Cir.).

United States v. Hagarty. (1968) 388 F.2d 713, 717 (7th Cir.).

United States v. Matlock. (1974) 415 U.S. 164.

United States v. Maxwell. (1996) 45 M.J. 406, 422 (C.A.A.F.).

United States v. Milian-Rodriguez. (1985) 759 F.2d 1558, 1563-64 (11th Cir.) .

United States v. Simons. (2000) 206 F.3d 392 (4th Cir.) .

United States v. Slanina. (2002) 283 F.3d 670, 676-77 (5th Cir.) .

Warden v. Hayden. (1967) 387 U.S. at 306-07, 294.

Whitman, M. and Mattord, H. (2005) *Principles of Information Security, 2nd Ed.*, Course Technology, Boston, MA.