Global Information Assurance Certification Paper

Mission Impossible: Warrants in the New Millennium

Deborah A. Orr
Version 1.2e
May 20, 2001

A. Introduction
B. Crafting The Affidavit

I. The Expertise of the Affiant
II. Applicable Law(s) & Definitions
III. Description of Property to be Searched or Seized
IV Description of the Location of Evidence to be Seized or Intercepted
V. History and Probable Cause

C. Execution of the Warrant

I. Warrant Types
II. Design Considerations
III. Method of Intrusion

a) ISP Interception
b) Keystroke Monitors
c) Trojans and Web bugs
c) Carnivore
e) DIRT
f) TEMPEST Attack

D. Summary

A. Introduction

In the days of cybercrime and cyberwar, the barriers to capturing evidence are not vicious dogs, booby trapped doors or secret hiding places. Today, law enforcement must also be able to overcome intrusion detection mechanisms, encryption and spoofed identities. The evidence may be obscured by jurisdictional obstacles or stored on the property of unrelated and unwitting victims. It would be simple if agents could simply fight fire with fire and hack the suspect system but the US legal system takes great care to ascertain that enforcement does not intrude on citizen rights to privacy.

For this reason, retrieval of electronic data generally requires a warrant or order signed by a judge who presides in the jurisdiction in which the crime is occurring. To obtain such an order, probable cause must be established via a sworn affidavit. This affidavit must describe with great specificity the nature of the evidence (including all forms in which it may exist) and the location(s) which is ***likely*** to lead to discoverable evidence. Hence, the first obstacle presents itself. **Where and what is the evidence?** Things are not always what they seem in cyberspace and the term "moving target" takes on a whole new meaning.

Assuming that the judge is convinced that a crime is occurring and that the evidence and it's location has been adequately described, the agent will encounter the second obstacle to obtaining the coveted warrant. **How can the evidence be retrieved?** Brute force will not capture the prize in today's arena. This is truly a battle of wits and the side with the technological edge will be the victor. First, a plan must be devised to minimize or eliminate collateral intrusion. In cyberspace, it is often very difficult to avoid encroaching on an innocent bystander's space, especially when the evidence has been deliberately commingled with it. If an affidavit can be sculpted which adequately overcomes the above challenges, a warrant will most likely be issued. A signed warrant, however, does not mean that beneficial evidence can be gleaned. Retrieval may include seizure of tapes, discs or hard drives but might also include ongoing surveillance (a wiretap) and the challenge of invisibility. Storage media is a simple matter of forced seizure but a wiretap amounts to a court sanctioned hack which must be skillfully designed. Finally, consideration should be given to the possibility that anywhere in the process of manipulation, the evidence could self-destruct just like on "Mission Impossible"!

B. Crafting The Affidavit

The affidavit is a lengthy document which outlines the expertise of the affiant, the description of the property to be searched, the description of all property to be seized, a history outlining the probable cause and a proposed execution plan . Separate warrants should be obtained for each location or computer to be searched. This paragraph will focus on the assertions and clauses contained within the affidavit which are unique to computers and digital evidence.

I. The Expertise of the Affiant

In addition to standard training and experience, the swearing agent should include training and experience in cybercrime and computer forensics, security and analysis as well as membership in related organizations.

II. Applicable Law(s) & Definitions

The application should site the laws applicable to the essence of the affidavit and order being sought and how they they relate to the suspected crime and the authority being sought. While most judges are familiar with computer issues, it may be beneficial to define certain relevant terms, especially when describing technical terms related to execution of the warrant.

III. Description of Property to be Searched or Seized

The Privacy Protection Act (PPA) basically prohibits law enforcement from "searching for or seizing" authored materials or work product intended for communication to the public or intellectual property. Since personal computers are commonly used to produce First Amendment materials, care must be taken to use language which narrows the scope as much as reasonably possible by:

Describing the general class of information to be seized (i.e.: All records *relating to violations of 21 USC - Applicable section*) between *Certain Dates,* including *types of evidence* (i.e.: phone records, address books, identifying information of specific activities or transaction), and *documents recording suspect travel, all bank records, checks, credit card bills, account information* or *other financial records.*

Defining "records and information" to include any electronic or magnetic storage device including floppy diskettes, hard disks, CD ROM's, backup tapes, printer buffers, smart cards, memory calculators, biometric authenticators, optical discs, pagers, personal digit assistants, or any other criminal identifying information including any handmade, mechanical or photographic form.

Describing reasons for *physical removal* of computer equipment since technically the hardware often serves as merely a storage vehicle for the information which the agents have probable cause to seize. For this reason, the affidavit should describe probable cause that the equipment itself is an instrumentality to or contraband of the crime.

Warrants on the hardware of innocent bystanders or for information which is disguised or commingled becomes more difficult to accurately describe. While specificity is crucial to defending a challenge to the warrant, courts have recognized the complexity of some criminal enterprises and have held that "search warrants may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit". Also, if protected materials are incidentally seized, an effort to return such materials as soon as possible after discovery will further defend PPA violation claims.

IV Description of the Location of Evidence to be Seized or Intercepted

Digital storage and communication augmented by the ingenuity of criminals has made the location of evidence harder to pinpoint or describe.

a) Jurisdiction

Federal rule requires search warrants to be sought in the district where the property to be searched is located. Since computers can be accessed remotely, criminals do not need to be at the scene of the crime or in possession of the evidence. They can exercise control across continents and deliberately store data on servers located in uncooperative countries. For this reason, investigations may involve coordinated efforts of foreign governments arranged through the Office of International Affairs. The need for such international cooperation may delay or otherwise hamper investigation due to inconsistent law and investigative techniques. When international cooperation is unwise or unlikely, agents may need to convince a judge that more intrusive measures such as wiretaps, backdoors or tempest attacks are warranted due to evasive tactics

employed by the suspect.

Additionally, if an order to remotely access a computer is sought, law enforcement may need to determine the exact location of the computer via server subpoena and convince the judge that such intrusion would not constitute a criminal act in the country where the computer is located. Transborder obstacles could also occur in the US when an activity is legal in one state but not another, such as gambling.

b) Disguised/Commingled Evidence

The Fourth Amendment requires that the warrant must describe the evidence clearly enough that no discretion is left to the agents and the description cannot be overly broad that it might include irrelevant data. Since evidence can encrypted or otherwise disguised or embedded in an apparently innocent program, the warrant language must be carefully chosen and should include permission to retrieve "any form" of it. Also, the encryption type can affect the point of interception. For instance SSL information might decrypted on either end of a communication while public key encryption might best be retrieved by a man in the middle attack.

c) Evidence Stored on a Victim System

If possible, when evidence is stored or manipulated on a compromised computer, the owner's permission should be sought. This may not be advisable or possible if the victim computer is in another jurisdiction or permission is denied. In any event, contemporaneous notification of the intrusion would most likely be required.

V. History and Probable Cause

How do we establish probable cause that a storage device or electronic communications are likely to reveal admissible evidence? Once the warrant is justified, how do we convince a magistrate that we need to hack into the target system and perhaps upload a virus or maybe break into a residence to install a device? Lastly, how do we filter data so that only admissible evidence is obtained. These areas will be explored in this section.

a) Admissions against interest:

Let's start with establishing probable cause. One of the easiest ways to establish probable cause in a computer crime is by obtaining "admissions against interest" in the seemingly anonymous environment known as the world wide web. It appears that many cybercriminals feel safe conducting illegal activity via commercial websites or bragging about their prowess to peers. Depending upon the crime, the investigator can look for and document admissions in various locations. Particular attention should be placed on documentation which make the admission "stick" to the subject of the warrant.

Websites - Crimes where an illegal commodity is being sold, such as drugs or pornography, can often be documented by basic search engine queries (http://www.dogpile.com) for commercial websites. Such websites may contain names of persons, ordering and email information, fraudulent claims and security measures utilized in the safeguarding of identity or credit card transactions. It is very important to establish that the suspect has control over the content if an admission is to be established.

Various foot printing techniques are crucial to any cyberinvestigation for both evidentiary and surveillance purposes. If the website utilizes their own domain name, a "who-is" lookup can provide administrative and billing contacts along with their address, phone number, email and server. Various DNS lookup tools and utilities can be found that assist in providing information about the target, their (network) location, there server etc.
(http://www.samspade.org/t/).

Analysis of HTML source code can often provide useful information, especially regarding links and potential co-conspirators. Mirroring utilities are available to limit the investigator's exposure while allowing thorough analysis. (http://softbytelabs.com/BlackWidow/)

A commercial website is also an open invitation to establish communication with the perpetrator which can lead to recorded phone conversations and email analysis. The

investigator should understand that footprints can be left whilst navigating cyberspace which may include server log files, header packages, web bugs, cookies and more. Whenever browsing target websites, an anonymizer should be used to assure that the watched does not become the watcher (http://www.anonymizer.com). Criminals make it their business to avoid law enforcement detection so don't underestimate their level of technological expertise.

Newsgroups - Hackers, pornographers and drug traffickers find their peers on newsgroups. Here they can establish contacts, ask for help in devising attacks, reveal clues to their identity or brag about their illegal accomplishments. For this reason, monitoring newsgroups on related subjects can be very fruitful. Such searches can be done at http://groups.google.com/

Chatrooms - Child molesters, rapists and kidnappers frequently stalk their prey in chatrooms. Some merely conduct surveillance since the average user is oblivious to the dangers lurking on the internet and will reveal their name, location, habits and/or lifestyle to chatroom acquaintances. Others will attempt to establish relationships and instill trust before luring the victim to a rendezvous location. Investigators can often spot inappropriate or leading chat and turn the tables by portraying a vulnerable victim. In these instances email and personal meetings can be encouraged where a simple arrest and/or seizure of hard drives or email may be enough evidence to prosecute.

Emails - Fraudulent schemes such as investment rip-offs and illegal distributors of prescription drugs are notorious for stripping email addresses from newsgroups and sending unsolicited promotions to them. In such cases, admissibility will rely on the ability to prove that the defendant authorized or made such statements to overcome hearsay rules.

b. Digital Footprints - Another way to establish probable cause is to analyze digital tracks that may be left by perpetrators of crimes. This can be done a number of ways.

Intrusion Detection Devices - Log files created by softwares such as Black Ice or Zone Alarm will often provide IP and DNS information of intruders attempting to scan ports prior to an attack.

Packet Headers - Packet analysis can provide valuable clues to the originating computer but spoofing must always be considered. Less organized criminals such as stalkers or sexual offenders are probably not as computer savvy as a sophisticated drug operator or a computer "enthusiast".

Log Files - Server logs can provide valuable information regarding who's computer made access to what server files on which occasions.

A good directory with links to numerous databases and search resources is: http://www.freeality.com/

Various online tools to assist in recognizance are located at: http://www.cotse.com/security.htm

---

C. Execution of the Warrant

The agent must learn as much as possible about the target computer's hardware, software, operating system & network configuration. Many factors will affect the type of warrant to be sought and the retrieval method which will prove successful.

I. Warrant Types- The type of warrant requested will depend on the specifics of the case:

a. No-Knock warrants -Generally warrants and agents are announced prior to the execution but in cases where agents are in danger or evidence will be destroyed (such as with computers), 'No-Knock" warrants are justified. Due to the labile nature of computer data, a No-knock warrant should be requested for any computer seizure to avoid destruction of evidence.

b. Sneak and Peek Warrants - If a showing can be made that notice should be delayed, a "Sneak-and-Peek" warrant might allow agents to break into a location, search a computer and leave no notice that entry was made. This can help to identify system security and passwords for future wiretaps.

c. Real-time electronic surveillance - The first known police wiretaps were executed in the 1890's (20 years after Bell's first phone call). Today, wiretaps are governed by the "Wiretap Statute" (Title III 18 USC 2510-22) which addresses the content of communications *in transit* and the "Pen & Trap" statute (18 USC 3121-27) which tracks incoming and outgoing phone numbers. The first internet wiretap was authorized in 1995 and operation assistance requests rose 18 fold between 1997 and 1999 to 1,350 full scale wiretaps in 1999. In fact permission to intercept the full content of email communication (which requires only probable cause of a federal felony) can be authorized by "any attorney for the government" and is easier than obtaining permission for a phone tap.

Title III focuses on "protected" communications and computer surveillance will revolve around one of six "**exceptions**":

1) **Interception authorized by a Title III Order**- A Title III Order is authorized by a Federal District Court for up to 30 days. The affidavit must show probable cause that interception is likely to lead to discoverable evidence of a predicate felony offense.

2) **Consent of a Party to the Communication**- This exception authorizes interception when one of the communicators consents to the interception. As previously mentioned, the seemingly anonymous nature of the internet makes it easier for agents to establish themselves as one of the "consenting" communicating parties. When a hacker loops through compromised computers to commit a crime, the compromised computer is *not necessarily a party* to the communication. In such cases, agents might consider alternatives to victim consent to prevent Title III challenges.

3) **The Provider Exception** - The service provider, under this exception, may intercept or monitor communications on their equipment for the purpose of combating fraud or protecting their rights or property. Agents will most often encounter resistance by the ISP to conduct surveillance without court intervention and rightly so. This exception exists so that the provider can protect *themselves* and not as a blanket authority to intervene in unrelated crimes against other parties. This does not, however, preclude the provider from independently monitoring/intercepting hijacked services and report their findings to law enforcement.

4) **The Extension Telephone Exception** - Title III protection excludes subscriber use of any facility furnished by the provider or any facility used by the provider or law enforcement during the regular course of business. The law enforcement exception should not be misinterpreted to avoid warrants as courts have held that the telephone exception is closely linked to the consent exception and that routine monitoring of ***all*** calls into a police station or prison would qualify but monitoring of one target's communication would not.

5) **The Inadvertently Obtained Exception** - One exception to Title III protection is when "a provider inadvertently obtains communication which appears to pertain to the commission of a crime and divulges such to law enforcement." This exception has not yet been tested in court.

6) **Accessible to Public Exception** - Many of the previously described ways of obtaining probable cause are permitted by the exception allowed in 18 USC 2511(2)(g)(i), which allows any person to intercept an electronic communication which has been configured to be readily accessible to the public (such as webpages, newsgroups & chatrooms).

Note: There is some confusion regarding when communication is "intercepted" (i.e.: during recording, when recording is physically retrieved or when recording is seen or heard). Most courts have held that interception occurs only at the time of transmission and that any subsequent retrieval would be obtaining access to "stored" communication. Since Congress clearly intended "stored voice communications" to be protected, for consistency, it is recommended that a Title III order be obtained when obtaining "stored electronic communications".

II. Design Considerations

a) Commingled Evidence

If discoverable evidence is commingled with privileged evidence, a plan must be presented to the judge to screen out privileged evidence. Such review becomes especially relevant when evidence is commingled with

physician patient files, attorney work product or author freedom of speech or when the perpetrator has surreptitiously stored evidence on vulnerable systems. Failure of the government to attempt to identify First Amendment materials could deprive them of a "good faith" defense should the warrant be challenged. A proposed plan could include in-camera review by the judge, review by a court appointed third party or a privileged team unrelated to the prosecutor. The notorious FBI "Carnivore" software is capable of *automatically screening and filtering* privileged data while the warrant is being executed.

b) The Use of Cryptosystems - If the target uses PGP or SSL, where and how to retrieve the data becomes important and a sneak and peek warrant could be justified to determine if the target hard drive is encrypted, email is stored encrypted, vpn is used, passwords can be cracked etc. Since most readily available encryption software cannot be easily decoded without the key, a method to bypass encryption might need to be devised.

c) Intrusion Detection/Firewall Bypass - The wide availability of Intrusion Detection and Firewall software can inhibit a stealth attack and must be considered in execution design. If necessary, vulnerabilities can be identified and exploited in most protection software and IP spoofing or DoS attacks can often assist in penetrating harware firewalls. (http://www.megasecurity.org/Firewall_related.html)

III. Method of Intrusion

a) Hardware/Software seizure - Examination of storage devices requires a trained specialist to capture all the digital evidence which exists and preserve it in a manner that documents authenticity. Potential evidence can exist in printer buffers or memory, monitors and authentication devices as well as CD-ROMS, removable drives and floppy discs. Files may also be hidden in partitions, programs, graphics or remote computers and it is the forensic analyst's job to locate and preserve them.

b) ISP Interception - Obtaining data from the Internet Service Provider can be the beginning or the end of the line depending on whether the perpetrator has hijacked another person's account. Since decryption occurs on the host computer, ISP interception will probably not yield discoverable evidence if email is encrypted but with SSL (Secure Socket Layer) encryption occurs at the Transport Layer and the ISP might be a viable choice. Further, the level of information sought will dictate the type of order used to compel disclosure by the ISP:

Subscriber Information (requires a **subpoena**)	**Transaction Information** (requires a **court order**)	**Content Information** (requires a **search warrant**)
Name	Log On & Off times	Content of emails
Address	Time on Line	Content of Files
Telephone Number	Sites Visited	Content of Downloads
Billing Information	Newsgroup Subscriptions	
Account Start Data	Credit Card Numbers	
Account Status	Names of correspondents in email & newsgroups	

* This chart based on information provided by the National White Collar Crime Center course: The Internet as an Investigative tool

b) Keystroke Monitors - Keystroke monitors record keystrokes and can save them to a hidden file for subsequent seizure or can periodically send them home to circumvent dumps upon discovery. In the case of Nicodemo Scarfo, son of the Philadelphia syndicate godfather, the government obtained permission to break into his residence to plant a keystroke monitoring device on the target computer to capture everything the suspect typed, including passwords for encrypted files stored on the hard drive. Alternatively, if a vulnerability can be identified in the target computer, it may be possible to upload a trojan containing a key stroke monitor or a web bug which "phones home" but the risk that the intrusion will be discovered is an associated consideration.

c) Trojans and Web bugs - If target security is vulnerable, malicious code can supplant the need for monitoring hardware in Title III orders. The same types of attacks used to commit computer crimes could be justified in various types of warrants.

d) Carnivore - Carnivore is the FBI's most recent version of wiretap software. It is a high speed packet sniffer which has met with much resistance from privacy groups primarily based on the "wide net" cast by it's predecessor - Omnivore. The improvements of Carnivore allow enforcement to fine-tune the system to capture only the sources and recipients of the target's email at the ISP level (which is essentially the same as traditional trap and trace devices). The major problem with Carnivore is that it is easily thwarted by encryption.

e) DIRT - (Data Interception Remote Transmission) - DIRT is a software only available to law enforcement and military which is similar to Back Orifice and closely approximates a wiretap. There is currently no defense against the use of this software

F) TEMPEST Attack - Tempest (Transient Electromagnetic Monitoring Pulse Standard) is a classified government program based on the knowledge that all electronic devices emit low level electromagnetic radiation that can be remotely captured and later displayed. Compromising emanations radiate from many sources including computer monitors, tape drives, scanners, printers and power cables which can be captured from a van parked on average about 300 yards from the source. There is no way to detect Tempest surveillance and it is unclear whether a court order would be needed to collect Tempest information. Depending on the location, protection from capture could cost millions.

D. Summary

Clearly, warrants for "cyberevidence" require special considerations in their preparation and execution. With the rise of internet and computer crimes, such warrants are becoming increasingly necessary to agents. Unfortunately, the dynamic nature of electronic communications makes it impractical to create a blueprint for obtaining warrants or enumerate all of the ways in which one can be executed. For this reason, trained analysts should assist agents and prosecutors in both the preparation and the execution of the warrant. In designing a strategy, one should realize that while the playing field has changed, the rules have not! Laws exist which protect rights to privacy yet authorize warranted access by enforcement.

In most cases, analogies can be made between physical and electronic searches which have assisted courts in extrapolating existing laws into uncharted territory. For instance, encryption is similar to a locked door. An order to obtain evidence behind the door implies authority to "break" the door down (or search for keys to decrypt). Hiding evidence on a victim computer might be compared to burying a body in your neighbor's yard. A separate warrant should be obtained for the remote location. As computer crimes evolve, successful arguments will set precedence which will then be circumvented by the ingenuity of the criminal mind.

Hence, the role of trained computer security specialists in detecting and prosecuting cybercrime will forever be a challenging and rewarding one.

E. References:

1) Computer Crime and Intellectual Property Section, United States Department of Justice - **Search and Seizure Manual: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.** January 2001 - http://www.cybercrime.gov/searchmanual.htm

2) Computer Search and Seizure Working Group, US Dept. of Justice - **Federal Guidelines for searching and seizing computers.** April 24,2000
http://www.usdoj.gov/criminal/cybercrime/search_docs/toc.htm -

3) Ellerman, Sarah - **Beware the Keystroke Cops.** Sept. 7, 1998 - http://www.techweek.com/articles/9-7-98/paranoia.htm

4) Kubiszyn, Margaret Smith - **Legal Controversy and the FBI's "Carnivore" Program**. December 2000 - http://www.gigalaw.com/articles/kubiszyn-2000-12a-p1.html

5) Schwartz, John - **Fighting Crime Online - Who is in Harm's Way**. Feb 12, 2001 - http://www.infowar.com/law/01/law_021201e_j.shtml

6) The President's Working Group - **The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet**. March 2000
http://www.usdoj.gov/criminal/cybercrime/unlawful.htm

7) Meeks, Brock N - **FBI's Carnivore has partners**. October 17, 2000 - http://www.msnbc.com/news/477749.asp

8) Krebs, Brian - **FBI Hacks Suspect's PC to Monitor Alleged Mob Activity**. Dec. 6, 2000 - http://www.infowar.com/law/00/law_120600c_j.shtml

9) Jones, Frank - Nowhere to run .... **Nowhere to hide.... The vulnerability of CRT's, CPU's and peripherals to TEMPEST monitoring in the real world...** 1996 - http://www.spyking.com/c_tempest.html

10) The National White Collar Crime Center - **The Internet as an Investigative Tool**. March 2000, 3rd Edition