Going for the throat: Carnivore in an Echelon World[1] - Part I

Talitha Nabbali, and
Mark Perry,[2] University of Western Ontario

Carnivore is a surveillance technology, a software program housed in a computer unit, which is installed by properly authorized FBI agents on a particular Internet Service Provider's (ISP) network. The Carnivore software system is used together with a tap on the ISP's network to "intercept, filter, seize and decipher digital communications on the Internet". The system is described as a "specialized network analyzer" that works by "sniffing" a network and copying and storing a warranted subset of its traffic. In the FBI's own words "Carnivore chews on all data on the network, but it only actually eats the information authorized by a court order". This article, in two parts, will provide an overview of the FBI's Carnivore electronic surveillance system. The Carnivore software's evolution, its 'prey' and the system's relationship with Internet Service Providers will be the focus of the study. (Although the FBI's Carnivore surveillance system is now officially called DCS1000, as the surveillance system is more commonly referred to as "Carnivore", that term will be used throughout). Also addressed in the article are misconceptions about Carnivore, publicly available sniffer programs, Carnivore's functionality, methods to counter Carnivore as well as the software's limitations. In addition, the pertinent American law allowing for wiretapping and electronic surveillance as well as programs and policies outside the United States regarding electronic surveillance are surveyed, and an overview of ECHELON, the global interception and relay system, is provided. The aim is to provide the paper's readers with a better understanding of these surveillance systems: naturally, only through an in-depth knowledge can the benefits and dangers they present for the public (government), private (individual communications users) and technical industry (ISPs) be understood.

A. Introduction

With the rise in the number of crimes involving the exploitation of computers, networks and databases, law enforcement agencies need to conduct electronic surveillance in order to acquire evidence and prevent criminal activity using these technologies. To aid in the electronic surveillance of the Internet, the Federal Bureau of Investigation (FBI) developed the Carnivore software system.[3] However, the development of technologies to intercept and record electronic traffic, whether phone or data networks, offers intelligence agencies additional techniques for the interception of communications of interest.[4]

The FBI maintains Carnivore allows the FBI to assist Internet Service Providers (ISPs), who are complying with court orders, to intercept electronic communications, and that Carnivore has been implemented in such a way as to discriminate between Internet use by a criminal suspect and use by innocent members of society. It has the unique "surgical" ability to intercept and to collect subpoenaed communications while ignoring those whose interception is not authorized.[5] In other words, Carnivore serves to limit accessibility to electronic communications to those specified by a court order. [6]

Carnivore is a surveillance technology, namely a software program housed in a computer, which is installed by properly authorized FBI agents on a particular ISP's network. The Carnivore software system is used together with a tap on the ISP's network to "intercept, filter, seize and decipher digital communications on the Internet".[7] The system is described as a "specialized network analyzer" that works by "sniffing" a network and copying and storing a warranted subset of its traffic.[8] In the FBI's own words "Carnivore chews on all data on the network, but it only actually eats the information authorized by a court order".[9]

The FBI views Carnivore as an asset for safeguarding Americans and, more specifically, the Internet against criminals. The agency fears that without a system like Carnivore, law enforcement agencies would have no control over the Internet and would thus allow the World Wide Web to become a safe haven for criminal activities and communications. However, the FBI's viewpoint of Carnivore is not a universal one. From the perspective of both the technology industry and individual Internet users, surveillance systems like Carnivore are invasive tools that allow government agencies to interfere with and intrude excessively

Computer Law & Security Report Vol. 19 no. 6 2003 ISSN 0267 3649/03

into their daily activities.[10] Individuals fear that Carnivore impinges on their right to online privacy and security. As technology advances, future versions of Carnivore will be more comprehensive and be capable of new techniques such as simply isolating encryption keys, giving the potential for both the government and technology savvy individuals to read more of our electronic communications.

Invasion of privacy and extended search and seizure powers for the state are a great concern. The technology industry faces a catch-22 situation with the usage of surveillance systems like Carnivore, the industry, especially Internet Service Providers (ISPs), must both satisfy their customers and adhere to the demands of law enforcement agencies in order to avoid commercial failure or enforced shutdown. By allowing Carnivore to be used on its system, an ISP risks upsetting and losing customers that are concerned with their privacy. However, by refusing to allow Carnivore to be deployed on their network, ISPs risk a legal battle with the government, which may lead to a shutdown of their operations. Satisfying both customers and the government is not the only problem: ISPs are also concerned that the use of Carnivore can be detrimental to their systems. Since the FBI refuses to release the technical details of the Carnivore system, ISPs fear that they are playing Russian roulette every time they install a Carnivore system on their network, as they cannot predict how Carnivore will interact with their operating environment. Apart from customer resistance, it is primarily fear of technical conflicts that has stimulated the technology industry to oppose Carnivore. ISPs are naturally wary of installing hardware or software of unknown provenance into their live system environments, as the potential for disruption of their systems and the attendant economic loss is very real.

This article provides an overview of the FBI's Carnivore electronic surveillance system, in particular Carnivore's evolution, its prey and the system's relationship with Internet Service Providers. Furthermore, the misconceptions about Carnivore will be addressed. This article will also survey publicly available sniffer programs, examine Carnivore's functionality, and expose methods to counter Carnivore as well as consider the software's limitations. Another aspect of such systems that are used in law enforcement is to see them in the larger context of spy software, epitomized by the infrastructure known as ECHELON. It should be noted at the outset, however, that some of the information provided is speculative and from hard to verify sources, as the nature of the beast is obfuscated by United States security concerns.[11] Nonetheless, the article will provide insights to the Carnivore surveillance system and ECHELON. Only through knowledge of their operations can the benefits and dangers of such surveillance systems for the public (government), private (individual Internet users) and technical sectors (ISPs) be assessed.

B. Carnivore's evolution

The FBI's Carnivore software system has generated public outcry.[12] However, long before the creation of Carnivore, the FBI had the capability to capture email from targeted sources. In order to understand the Carnivore online detection software system, it is essential to understand its predecessors.

The FBI's first online detection software dates back to at least January 1996.[13] It is widely believed that it was based on publicly available commercial software developed by a company specializing in network packet tracking. Many believe the software was WildPackets Inc.'s EtherPeek, an ethernet network traffic and protocol analyzer.[14] However, as the FBI has classified all information relating to its first online detection software as "secret", no verifiable information has been disclosed about its development.

Long before the creation of Carnivore, the FBI had the capability to capture email

Omnivore, the FBI's second online detection software, is the direct predecessor to Carnivore. The software was created because the FBI deemed its original online detection software to have "deficiencies that rendered the design solution unacceptable".[15] The FBI's Omnivore surveillance software was commissioned in February 1997 and was created by an unknown contracted source in collaboration with the FBI's Data Interception Technology Unit (DITU) and Electronic Surveillance Technology Section (ESTS)[16] at a cost of US$ 900 000.[17]

According to the FBI, the goal of Omnivore was to allow American governmental agencies to fulfill their need to capture SMTP traffic based on username, and print such emails in real time.[18] Consequently, Omnivore was designed to sniff through email traffic traveling over a specific ISP's network as to capture emails from a targeted source. Omnivore then saved the captured emails to either a 8 mm tape-backup drive and was also able to print them in real-time.

Omnivore's functions are almost identical to those of its successor, Carnivore. Like Carnivore, Omnivore was deployed on an ISP's network that

regularly handles a suspect's data. Once installed on an ISP, Omnivore captured TCP/IP application data traveling past its contact point. As TCP/IP application data was captured, Omnivore wrote a buffer of packet data to a shared memory area. As the memory area began to fill, Omnivore sifted through the information collected, applying user-defined filters to the buffered packet data. All packet data fitting the filter criteria was written to a storage medium (either a Zip drive or a Jazz drive) or to a printer while the rest of the data collected was discarded.

The first release of Omnivore was made available to the FBI as early as February 15 1997.[19] However, it was only in October 1997 that the first non-beta version of the Omnivore software was released.[20] Omnivore is believed to have been deployed a number of times between February 1997 and June 1999 when it was retired in favor of the more comprehensive DragonWare Suite.[21]

Omnivore was created for the Solaris X86 platform, but the Solaris X86 platform did not support a variety of popular commercially available hardware. Thus, deployment of Omnivore was slow, difficult and time consuming.[22] Consequently, in September 1998 the FBI devised the "Phiple Troenix" project (a spoonerism of the phrase "Triple Phoenix").[23] The goal of Phiple Troenix was to migrate the then present Internet collection system (Omnivore) "from a Solaris X86 platform to a Windows NT operation system" in order to facilitate "the miniaturization of the system and the support of personal computer (PC) equipment."[24]

Omnivore was quickly ported to run on Windows NT machines with a service pack of 3 or higher and given the code name "Carnivore". The total cost of the project was estimated at about US $800 000, which included the rewriting of Omnivore for the new operating system and the training of FBI agents and National Infrastructure Protection (NIPC) personnel on how to make use of the new software.[25]

Carnivore is thus the FBI's third generation of online-detection software, and a great improvement over Omnivore because more than simply scanning email traffic, the software suite is capable of reconstructing the Web pages surfed by someone under investigation.[26] Furthermore, Carnivore is more user friendly than Omnivore since it has a Windows-like user interface, provides remote control access, offers immediate download of current archive data and allows archive media without stopping collection or losing IP packets.

Carnivore is part of a software triad known as the DragonWare Suite (also known as DragonNet). The DragonWare Suite consists of Carnivore in addition to two other software programs named Packeteer and CoolMiner. Both Packeteer and CoolMiner programs take in the data intercepted by Carnivore. Packeteer reassembles packets into cohesive messages or Web pages while CoolMiner, a data-mining tool, allows for the extrapolation and analysis of data found in messages. Although, both these programs are believed to have been developed by contracted sources, the FBI has released no substantive information about either of the two programs.[27]

The first version of Carnivore dates back to September 1999 when version 1.2 of Carnivore was released.[28] Apparently Carnivore 1.2 retrieved too much data, botching investigations due to "digital indigestion".[29] Therefore, in March 2000 it was replaced with Carnivore 1.3.[30] It was only on June 16, 2000 after the FBI finished beta testing of Carnivore 1.3.4 that Carnivore was approved for operational deployment.[31] Although Carnivore 1.3.4 is the version used for surveillance operations, the FBI admits that versions 2.0 and 3.0 of Carnivore have been developed as part of the "Enhanced Carnivore Project" which began in November 1999 with an operational budget of US $650 000. It is believed that Carnivore 2.0 has the ability to display captured Internet traffic and extrapolate results directly from data without using either Packeteer or CoolMiner programs and is compatible with Windows 2000,[32] whereas Carnivore 3.0 is rumored to be capable of intercepting voice over IP communications.[33]

The FBI's electronic surveillance and interception capabilities are continually under development. In November 2001, it was learnt that the FBI had created a computer virus that once inserted onto a suspect's computer could be used to obtain the cryptographic keys of that machines' users.[34] As Carnivore can only capture data after it has been transmitted over the Internet, at which point it may be already encrypted, the Carnivore detection software is useless against suspects who use strong encryption. The FBI's hope is that by capturing encryption key information from suspects they will be able to decipher encrypted information gathered by Carnivore and consequently prevent illegal activities and arrest criminals.

The virus developed by the FBI is known as "Magic Lantern". The Magic Lantern virus is either sent to a suspect's computer via email or the FBI can use known vulnerabilities in operating systems or

other applications to break into a suspect's computer and insert the Magic Lantern virus.[35] According to information leaked to MSNBC, "Magic Lantern installs 'key logging' software on a suspect's machine that is capable of capturing keystrokes typed on a computer. By tracking exactly what is being typed, critical key encryption information can be gathered and transmitted back to the FBI".[36] However, the FBI denies having used Magic Lantern and claims that the virus is nothing more than a "workbench project", unfit for deployment.[37] Magic Lantern is one of many enhancements currently being developed for the Carnivore electronic surveillance software. Magic Lantern and other enhancements to Carnivore are currently being made under the umbrella project name "Cyber Knight".[38] Few details regarding the "Cyber Knight" project have been released, however, it is believed that among the projects being developed is a data mining tool that sorts and matches data gathered using Carnivore and a database capable of matching files with their necessary encryption keys.[39] These projects are distinguishable from new proposals for a Total Information Awareness (TIA) system. Though TIA is more of a data mining and data collation operation than an intercept operation, and has undergone a recent name change to Terrorism Information Awareness Program, it remains a project with immense potential.[40] The development of the TIA project is being overseen by John Poindexter, the former national security adviser under President Ronald Reagan.[41]

On February 13, 2001, the FBI announced that they had given Carnivore a new name, DCS1000. Although, many reports suggested that the letters DCS stand for "Digital Collection System", the FBI maintains that DCS "doesn't stand for anything".[42] Furthermore, the FBI denies that the "name change stemmed from worries that the name "Carnivore" made the system sound like a predatory device made to invade people's privacy".[43] Nonetheless, it is widely believed that the FBI was eager to discard the name "Carnivore" since the Carnivore controversy has been one of the FBI's worst in their public relations in years.[44]

As Internet usage becomes widespread, the FBI has encountered an increasing number of investigations in which criminals use the Internet. In recent years, the Internet has been used to plan and execute criminal activity, in addition to being used as a means for offenders to communicate with their victims.[45]

The FBI maintains that the Carnivore system is needed to help combat acts of terrorism, espionage, information warfare, hacking, child pornography, serious fraud and other serious and violent crimes occurring over the Internet since such acts threaten the security and the safety of the United States and its people.[46]

C. Internet service providers (ISPs) and Carnivore

For Carnivore to be able to conduct electronic surveillance, it must be directly connected to an Internet Service Provider's network. Therefore, the FBI must receive technical assistance from an ISP's personnel when executing an electronic surveillance order.[47] Although ISPs are not thrilled by the fact that they must install foreign devices onto their network, such that the FBI can tap the IP packets of their customers, the Department of Justice's interpretation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 demands an ISP's cooperation.[48]

[A] court order authorizing the interception of communication shall upon the request of the application, direct that a telecommunications service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian or person is according the person whose communications are to be interception.

In accordance with Title III, a judge can sign two court orders; one authorizing the FBI to conduct the electronic surveillance and the other directing the ISP to provide the necessary assistance to the FBI.[49] Thus, Internet Service Providers are left with no choice but step back and let the FBI install mysterious Carnivore boxes on their networks.

Although the FBI possesses total control over the implementation and interceptions made by Carnivore, they maintain that their relationship with Internet Service Providers is far from dictatorial. The FBI asserts that they take many steps in order to guarantee that ISPs are aware of what is happening to their network and to assure the integrity and the security of the network is maintained.[50] For example, the FBI asserts that they have never installed a Carnivore box on an ISP's network without thorough consultation with the ISP's technical personnel.[51] According to the FBI, installation of a Carnivore box without the support and assistance of an ISP's personnel is foolish, if not impossible because Internet Service

The FBI maintain that their relationship with internet service providers is far from dictatorial

Provider's employees best understand the protocols and architecture of their particular network.[52]

However, many ISPs believe that they are in a better position than the FBI to comply with court orders authorizing electronic surveillance because they best understand their network and they have a dual duty to both produce information required by court orders and protect the privacy of their customers.[53] In regards to such claims, the FBI maintains that Carnivore is only used when an ISP is not able to fully and properly implement the court order; in all other instances the FBI states that they leave the interception to the ISP.[54] Nonetheless, in their statement to Congress the FBI asserts that Carnivore is superior to the commercially available sniffer tools that ISP network administrators might typically use for network administration.[55] According to the FBI, commercially available sniffers are the closest thing network administrators have to electronic surveillance devices, yet given that these sniffers were not designed as law enforcement electronic surveillance tools, they are not suited to law enforcement use. The FBI believes that given the differences in network protocols and header addressing information and their implementations by ISPs, data collection using commercially available sniffers can lead to the collection of a small amount of non-subpoenaed data. Thus, the FBI claims that resorting to commercially available sniffers cannot suffice from a law enforcement point of view for collecting court ordered information.[56] In other words, the FBI rejects that ISPs could sufficiently collect data using publicly available software and thus compels ISPs to deploy Carnivore on their networks. It seems that ISPs have no choice but to allow Carnivore's deployment on their network if they wish to avoid judicial problems. Thus, Internet Service Providers must cooperate with the FBI at all costs, even if this means giving up control of their network and sacrificing its integrity.

D. Misconceptions regarding Carnivore

Given Carnivore's notoriety, many misconceptions have arisen. These misconceptions range from far-fetched fantastical beliefs to slight departures from the reasonable. Here we address these misconceptions.

It has been said that Carnivore boxes have the capacity to shut down the Internet.[57] This is unlikely as even a malicious Carnivore box would damage only the part of the network to which it was connected, with traffic being routed around such damage. To shut down the Internet using attacking-Carnivore boxes there would have to be thousands of these boxes acting in unison positioned on ISPs as well as major Internet interchanges and second-tier peering points throughout the United States.[58] Moreover, these Carnivore boxes would have to contain attack software. Yet as Carnivore boxes are connected to a network by a bridging device they are physically prevented from transmitting data,[59] making an attack an impossibility. It should be noted that even if Carnivore's bridging device was disabled and Carnivore was capable of creating an attack on the Internet, once ISPs figured out that Carnivore boxes were causing the Internet "shut-down" they would only have to unplug the boxes from their network to rectify the problem.[60]

Many believe that by placing a Carnivore box on a given network that network's traffic slows down. This is not the case because Carnivore is a passive sniffer, thus it does not intervene with Internet traffic. Instead, Carnivore merely copies transmitted data as it passes.[61]

The misconception that Carnivore slows down electronic communications was further propagated in the wake of the terrorist attacks of September 11, 2001. During this period, Internet users worldwide experienced Internet and email delays. Many believed the culprit of the slowdown to be Carnivore, since it was heavily deployed during this period. In reality the slowdown had nothing to do with the heavy use of the Carnivore electronic surveillance system, it was caused by the SirCam worm which clogged email systems leading up to September 11, 2001 and the Nimda virus that infected networks worldwide on September 17, 2001.62

Carnivore works by decoding Internet traffic, looking for particular addresses and collecting data matching those addresses. The FBI asserts that Carnivore does not search Internet traffic looking for key words or particular content. Not only is Carnivore not designed for such searches, but US law also makes content-searching the communications of US citizens in this way illegal.[63] However, it is important to note that Carnivore does have the built-in capability to perform content searching namely its text filtering mode. The reason Carnivore has the power to perform content-searching is for the legal purpose of gathering web-based email, such as emails sent by services like Hotmail.com and Yahoo Mail.[64] Unauthorized wiretaps are illegal. In order for the FBI to get a court order to install a Carnivore box on a given ISP, they must specify exactly who are going to be monitored, what sort of data is to be

collected and the time span of the wiretapping operations. Furthermore, the Carnivore surveillance system was only designed for "surgical" wiretaps and it is therefore unable to conduct wiretaps of such a massive scope.

Carnivore does not capture electronic communications as such; instead Carnivore copies raw Internet packet traffic. Because Carnivore captures raw Internet traffic, it does not merely copy electronic communications, but also copies "checksums" that allow captured traffic to be checked for corruption and "sequence numbers" that prove that messages were captured without fragmentation.[65] While capturing raw Internet traffic itself does not prevent corruption, it allows the FBI to prove using checksums and sequence numbers that the recorded messages were not corrupted or fragmented during the transmission, capturing or copying process. By proving that no corruption or fragmentation took place, the communications captured by Carnivore will not be excluded on these grounds from being used as evidence in court.

There are strict laws in the United States regarding the use of wiretaps. One provision is that the wiretap order is only good for 30 days.[66] It would therefore be illegal for the FBI to permanently place a Carnivore box on an ISP's network and engage in wiretapping. This is in contrast to the United Kingdom where the tapping equipment is placed in all ISPs, but a court order is required to engage in the tapping operations.

E. Publicly available sniffers

The FBI's first electronic communication surveillance software is believed to have been a publicly available sniffer program, namely WildPackets' ethernet protocol analyzer and packet debugger; EtherPeek.[67] Many believe the FBI abandoned EtherPeek because of its limited surveillance capabilities. Presumably the FBI switched to a tailor made product so that it could conduct broader electronic surveillance. There are, nonetheless, many publicly available sniffer programs. Many of these sniffers programs are believed to be much stronger and more comprehensive than Carnivore. Thus, ISPs may want to be able to comply with court orders to intercept and conduct electronic surveillance using sniffer programs of their choice, providing they observe laws regarding electronic surveillance.[68] The FBI does not argue directly against ISPs having the right to choose their own monitoring equipment, but they do insist that only Carnivore complies with wiretapping and surveillance laws.[69]

Regardless, of whether Carnivore is the only sniffer software that adheres to American statutes regarding wiretapping and surveillance, in addition to the regulations for secure evidence, an overview of some of the existing publicly available sniffer programs may be illuminating.

Altivore is an open source program developed by NetworkICE which attempts to duplicate all Carnivore's features, including pen mode interception, full-content interception and IP address discovery. Altivore uses packet decoding techniques that allow for the collection of a sole stream of data, thus the program avoids violating the privacy of other network users not targeted by an investigation.[70]

NetworkICE hoped that Altivore would allow ISPs to comply with court orders requiring Internet monitoring without having to use the FBI's Carnivore software. Although, Altivore stirred up much publicity, the open source file altivore.c is no longer available because NetworkICE has been taken over by Internet Security Systems which has terminated the project.

SilentRunner is believed by some to be better than any other commercial sniffer and more comprehensive than Carnivore.[71] SilentRunner claims to analyze information from 25 different angles using algorithms instead of key searches to find target information. Furthermore, SilentRunner is able to recognize over 1400 protocols, including emails, Web pages, digital files, word documents and much more.[72]

Forensics Explorer claims that NetWitness provides a viable alternative to Carnivore because it allows an ISP to surrender only specific bits of information about a suspect that has been authorized by a court.[73] They further suggest that NetWitness can separate data to ensure strict minimal compliance with pen register or trap-and-trace orders and can later re-associate the original content of these messages if or when a court order for this information is issued.[74] Forensics Explorer maintains that since many believe that Carnivore collects more data than a pen register[75] or a trap-and-trace[76] order demands, "ISPs can use the NetWitness kit to stick to the letter of the law".[77]

WildPackets Inc.'s EtherPeek, Ethernet protocol analyzer and packet debugger, is believed to have been the FBI's first electronic surveillance software system. WildPackets Inc. maintains that EtherPeek conducts surveillance similar to a phone tap.[78] EtherPeek captures all data packets exchanged between nodes on an Ethernet wire

There are strict laws in the United States regarding the use of wiretaps

regardless of the hardware and software installed on the network.[79] Accordingly, EtherPeek monitors, filters and decodes data packets to expose core information.[80]

Many organisations are turning to wireless networks because they are easy to set up, move and they eliminate unsightly cables.[81] However, wireless computer networks pose a great security threat. A wireless network, also known as an 802.11b network or WiFi network has a built-in encryption system called Wired Equivalent Privacy (WEP).[82] Various weaknesses have been found in the algorithms making up WEP, the most serious described by Fluhrer et al.[83]

AirSnort and WEPcrack are wireless Local Area Network (LAN) tools that use the weakness of WEP described by Fluhrer, Mantin and Shamit to recover encryption keys.[84] AirSnort and WEPcrack operate by passively monitoring packets as they are broadcasted to compute encryption keys when enough packets are intercepted.[85] It takes approximately 100M-1GB of data in order to decipher encryption keys using AirSnort or WEPcrack. Once this amount of data is intercepted it takes the programs less than 1 second to decode the encryption password.[86]

F. The functionality of Carnivore

The FBI's Carnivore surveillance system is fundamentally a packet sniffer program that intercepts and examines IP packets as they pass on an Ethernet data stream. When a packet sniffer program, such as Carnivore is installed on a computer, the computer's network interface is set to "promiscuous" mode, such that it retrieves all information passing through the network interface regardless of the addressing information of the packets in question.[87] It is important to note that the amount of information retrieved by a packet sniffer depends entirely on where it is located on a network. A packet sniffer located on an isolated branch of a network will only retrieve a small segment of the network traffic, whereas a packet sniffer located on a network's main artery will retrieve almost all the data passing through the network.[88]

The FBI claims that Carnivore is placed such that it retrieves the least network data possible allowing for the fulfillment of the court order.[89] Furthermore, in order to prevent disruption to an ISP's network, Carnivore creates a copy of all the data that flows through the system at the intercept point, and processes the copied data rather than the original data.[90] After the full data stream is copied (including emails, Web sites visited, instant messages sent, FTP and all other network activity), the Carnivore box filters the data so that only packets that are authorized to be collected are maintained.[91] Carnivore accomplishes the filtering of collected IP packets by subjecting each packet to a series of tests looking for specific patterns. Depending on the failure or the success of these tests, packets are selected and recorded to memory, and subsequently copied to either a removable disk or a hard drive.[92]

A collection computer or Carnivore box is a personal computer running Windows NT or Windows 2000 and a C++ application that provides packet sniffing and filtering capabilities. More specifically, a Carnivore box consists of a single personal computer, which may be a laptop, with minimum requirements of a Pentium III processor, 128 MB of Random Access Memory (RAM), a disk drive capacity of 4 GB and either a Zip or Jaz drive to which filtered data is recorded for easy retrieval.[93] In addition, commercial communications software, a physical lockout program (to keep others besides the FBI from accessing the system), and a network isolation device (to make Carnivore invisible on the network) are installed on the Carnivore computer.[94]

1. Carnivore's filtering mode

Carnivore has six different filtering modes, which allow the FBI to intercept the data needed to fulfill court orders calling for the interception of Internet transmissions. These six different filtering modes can be joined by the Boolean 'AND' operand in order to guarantee that electronic surveillance is conducted efficiently. Carnivore's six filtering modes are:[95]

- **Fixed IP Filtering:** used when a target uses a computer with a fixed IP address.
- **Dynamic IP Filtering:** used when a target uses either RADIUS or DHCP to obtain an IP address.
- **Protocol Filtering:** enables the FBI to collect a target's TCP, UDP or ICMP data. The protocol filter has three different settings:
  - *Full*: which collects all packets from a specified IP address.
  - *Pen-mode*: which collects address information if such information is available (i.e. "To" and "From" addresses in SMTP email or IP addresses for FTP and HTTP traffic), replacing all other information with Xs.
  - *None*: which collects no data.

It is by choosing between the "full" setting and the

"pen-mode" setting that the FBI can specify whether its electronic surveillance will be restricted to transactional information (pen-mode setting) or will intercept both transactional and substantive data (full setting).

- **Text Filtering:** allows for the collection of data containing a specific text string. The text filter is used to capture web-based emails such as those sent by services like Hotmail.com and YahooMail.
- **Port Filtering:** allows for the collection of TCP or UDP traffic data. The port filter can be set to record data originating from a specific port, for instance, port 25 (SMTP), 80 (HTTP), 110 (POP3) or any other combination of ports of interest.
- **Email Address Filtering:** allows Carnivore to filter based on email addresses. To use email address filtering, both an email address and the proper mode of the email (SMTP or POP3) must be specified. If only a proper mode is selected, Carnivore will record every packet of the specified node traveling through the network on which the Carnivore box is installed, regardless of the email address of the sender or the receiver.

G. Counter-Carnivore measures

The FBI claims that the Carnivore electronic surveillance software system helps guarantee national security and prevent criminal activity facilitated by the use of the Internet.[96] Yet, many precautionary measures can be taken to prevent Carnivore, or other similar devices, from conducting effective electronic surveillance. Consequently, critics reject the FBI's claims that Carnivore can effectively prevent crime and guarantee national security. Instead, opponents of Carnivore believe that "Carnivore is a joke to anyone who deems themselves a hacker, cracker, computer-criminal or power user…. [since] countering Carnivore is simple, and only the foolish criminal would be caught by Carnivore."[97] The following are some simple ways to protect one's self from Carnivore and other similar surveillance devices.

Carnivore captures electronic mail by matching email addresses in the FROM and TO fields.[98] Thus, a simple way to prevent Carnivore from capturing your electronic communications is to change your name and email address when sending emails. By changing the name fields and the email field preferences in the options of your email software, Carnivore will never capture the emails you send or record that they were sent. However, it is important to realize that although forging an email sender can prevent Carnivore from capturing or recording outgoing emails, it cannot prevent Carnivore from detecting incoming emails as the receiver has to have the TO address present.

Email encryption is considered the easiest way to protect one's self against Carnivore's surveillance, since encryption products are readily available and are strong enough to prevent anyone from reading your email.[99] However, in the wake of the FBI's development of "Magic Lantern", a computer virus that installs key logging software to detect encryption keys, encryption as a counter measure against Carnivore's surveillance might not be foolproof.

By using an anonymous remailer, email traffic is forwarded in a form such that it is untraceable by law enforcement agencies. The most effective remailers use encryption. In order for encryption to be effective, messages must be encrypted numerous times. An anonymous remailer works by sending electronic communications to the first remailer, which decrypts the message once in order to discover the name of the next remailer along its path. The remainder of the message is still encrypted, so that only the next remailer along the path can further decrypt the message and send it to the next hop along the remailing path. This process continues, until the message reaches its final destination, where the message is decrypted for the last time to recover the original message.[100]

Anonymous remailers are an effective way to counter Carnivore-like systems, since if such systems are tracking the sender, they can only discover that he or she is using a remailer, but cannot discover the final destination of his or her messages.[101] Meanwhile, if Carnivore is surveying the recipient, it can only discover that received messages were sent by a remailer, but cannot determine who originally sent the message.

Carnivore can be defeated by attacking its inherent weaknesses. For instance, if you suspect that Carnivore monitors your electronic communications, it is possible to write a script that configures your computer system such that it sends an unending stream of emails, thus filling Carnivore's storage device.[102] Using one of the many random content generators on the Internet can create emails that appear meaningful.[103] By sending generated emails that appear meaningful, FBI agents are forced to examine every captured email individually in order to verify the authenticity of each message.[104] Such an

Critics reject the FBI's claims that Carnivore can effectively prevent crime and guarantee national security

attack on Carnivore will monopolize FBI resources rendering their surveillance less efficient.

SSL and SSH provide encrypted communications preventing third parties from monitoring communications. SSL and SSH connections will prevent Carnivore from monitoring what you are doing once surfing a particular site, since Carnivore will only see SSL or SSH gibberish.[105] However, an SSL or SSH connection will not prevent Carnivore from recording in Pen-Mode which websites are being accessed.[106]

Since SSL and SSH hardware is very expensive, SSL and SSH are only supported by a limited number of websites. Furthermore, SSL and SSH can only provide protection when properly used and account is taken of warnings. The server you are talking to provides mutual authentication, as to verify that it is indeed who it claims to be. Many times, warning messages are issued when using SSL or SSH, detailing that the connection to a server is not direct. If such warning messages occur, the SSL or SSH connection may not be safe, since a third party could have setup a server between your machine and the server to which you wish to connect. By installing a server between you and the SSL or SSH server, a third party can decrypt your traffic, record it, then re-encrypt it and re-route it back to the SSL or SSH server without your knowledge, making the SSL or SSH connection ineffective as a counter-measure to Carnivore's surveillance.[107]

Many companies, including Zero Knowledge, MessageRx, and mail2web[108], have also used SSL connections to provide services that allow web surfing anonymity. These companies guarantee web surfing anonymity by allowing their customers to establish SSL connections to their proxy servers. Once an SSL connection to a proxy server has been made, Carnivore will not be able to monitor which websites or activity has taken place. Carnivore will only be able to detect that the target of the surveillance operation is using an Anonymizer service.

Many ISPs seem to have little idea of the meaning of Carnivore, though some publish their policy for handling a Carnivore installation request.[109] These policies detail how an ISP will provide information to the FBI and what they will do in the face of a request to have Carnivore deployed on their network (not that they have much choice).[110] It is up to you, as an Internet subscriber, to decide whether to maintain your current ISP or choose another whose policies better suits your personal beliefs concerning the utilization of Carnivore.

H. Carnivore's limitations

Although the FBI has claimed that the Carnivore surveillance system will aid the Bureau in conducting investigations, Carnivore is not without shortcomings. The technology behind Carnivore is not able to record all Internet communications without problems. Slight problems in the collection of data can lead to a complete dismissal of all data collected by Carnivore for evidentiary purposes, so such limitations of the Carnivore system curb its usefulness. However, given that Carnivore and progeny offer the best electronic surveillance tools the FBI possesses, they have no choice but to hope that such software and implementations will be able to catch criminals and prevent unlawful activities. Listed are a number of limitations known to plague the Carnivore surveillance system.

Carnivore captures data after it has been transmitted over the Internet, at which point it is already encrypted. Thus, if a targeted suspect is clever enough to encrypt her Internet communications, the Carnivore surveillance system can only capture the gibberish created by the encryption process. The only salvation for the FBI is that encryption usually does not hide addressing information (sender and recipient addresses) and thus use of Carnivore in pen-mode will still bear utility.

The Independent Report details a number of weaknesses in Carnivore, which are summarized in the remainder of this section.[111] In order to intercept communications sent from web-based email accounts, like YahooMail and Hotmail, Carnivore must have explicit knowledge of the format of the provider's login messages. Such information will usually be given to the FBI upon request, and most web-based email accounts operate in similar manners. Nonetheless, Carnivore's processing of web-based email is a nuisance and a time consuming process. The FBI maintains that when collecting data on high-speed hard drives, Carnivore can handle data collection on networks with speeds up to 60 Mbps without dropping packets. However, Carnivore's collection rate drops to 15 Mbps when writing data to Jaz disks and drops to 5 Mbps when writing data to Zip disks. Considering the limiting factor for Carnivore's data collection is the input and output throughput of its storage devices and not a Carnivore box's CPU speed it seems unlikely that data collection rates will increase at the same rate as network traffic speeds. Thus, Carnivore will increasingly drop packets during collection, as network traffic speeds increase. Storage constraints seem to be one of the biggest challenges facing the FBI in regards to use of Carnivore. For example, if a

Carnivore box using a 2-GB Jaz disk to store data is collecting traffic on a network link that has a 25 Mbps traffic rate, the Jaz disk would fill-up in about 11 minutes. Not only would there be a need to change the Jaz disk every 11 minutes, but the input buffer would likely overflow during the time needed to change the disk, thus leaving valuable data uncollected. Even if 60-GB hard disks were used to store collected data, these would fill up in 5-6 hours if the network maintained a 25 Mbps traffic rate, creating a similar problem.

The Independent Report also notes even more fundamental problems.[112] Every FBI agent who uses a Carnivore box logs on as the "Administrator", rather than each individual agent possessing an individual identification number, so that every FBI agent accessing a Carnivore box has full control of all its resources. Thus, there are no security measures preventing the deletion or editing of any or all the files maintained on a Carnivore box by any agent with access. Once a Carnivore box is installed, it is physically under the control of the ISP. Although the Carnivore collection computer is left without monitor, keyboard or mouse, these ports are not covered or disabled. Thus, nothing prevents untrustworthy ISP personnel or others from connecting peripherals to the computer (and perhaps even lead to gaining control of the Carnivore box). Carnivore boxes are also susceptible to power failures. When power failures occur, Carnivore boxes cannot collect data. In addition, they lose all data stored in their buffers. Thus, a power failure could result in a loss of 0 to the maximum block size (128 kilobytes for fixed disks and 64 kilobytes for removable disks) of bytes of pre-collected data. Furthermore, a race condition within the Carnivore system prevents access to the Ethernet interface on reboot after a power failure. Consequently, Carnivore cannot start data collection automatically after a power surge. Instead, an FBI agent must manually restart the Carnivore system. Parameters for a given collection are stored separately from collected data. The only link between the parameters for a given collection and the collected data is the name associated with these files. Consequently, if these files become separated or renamed, it may become impossible to prove what settings were used to capture data, making collected data unusable as evidence in court. Timestamps are dependant on the collection computer's clock and its correct operation. The fact that timestamps are dependent on the clock in a Carnivore box can create a problem when multiple Carnivore devices are used in a data collection operation. If data from different Carnivore devices needs to be linked, differences in timestamps might prevent correlations.

It is easy to forge emails by simply reconfiguring an email system to use another email address. It is important to note that doing a simple reconfiguration of one's email system will not allow the reading of electronic communications destined to another but it will allow a person to impersonate another when sending emails.[113] Furthermore, through use of Trojan Horses, a hacker can both forge an email and send it from another's IP address. The use of Trojan Horses can fool Carnivore as well as law enforcement agencies and courts, since they make it impossible to tell who sent a given email. Consequently, innocent Internet users may be incriminated by evidence collected by Carnivore.

Talitha Nabbali BSc (Hons) Graduate 2002, University of Western Ontario and **Mark Perry,** Assistant Professor Faculty of Science (Computer Science) Faculty of Law University of Western Ontario; mperry@uwo.ca

FOOTNOTES

1 An earlier version of this article was presented at the Law Commission of Canada hosted conference In Search of Security: An International Conference on Policing & Security Montréal, Québec, Canada, February, 2003, under the title Going for the Throat: Techniques in Crime Control or Denial of Privacy.

2 Thanks to Michael McLaren, Rob Kitto, and Pam Krauss for their research assistance, funded in part by the Law Foundation of Ontario.

3 Although the FBI's Carnivore surveillance system is now officially called DCS1000, given the fact that the surveillance system is more commonly referred to as "Carnivore", this paper will use the term "Carnivore" when discussing the FBI's DCS1000 surveillance system.

4 Martin Bright, Ed Vulliamy, Peter Beaumont "Revealed: US dirty tricks to win vote on Iraq war" *The [United Kingdom] Observer* (2 March 2003), Guardian Unlimited http://www.observer.co.uk/iraq/story/0,12239,905936,00.html (date accessed 9 May 2003).

5 USA., Federal Bureau of Investigation, Carnivore Diagnostic Tool" Federal Bureau of Investigation, online: FBI <http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm> (date accessed: 3 July 2002) [hereinafter "Carnivore Diagnostic Tool"].

6 Ibid.

7 J. E. J. Jennings, "Carnivore: US Government Surveillance of Internet Transmissions (2001) 6 *Va. J.L. & Tech*. 10.

8 USA., Federal Bureau of Investigation, Internet and Data Interception Capabilities Developed by FBI, (Congressional Statement) by D. M. Kerr,(Washington, D.C.:24 July 2000), online: FBI <http://www.fbi.gov/congress/congress00/kerr072400.htm> (date accessed: 24 Dec 2002) [hereinafter "Internet and Data"].

9 R. Graham, "Carnivore FAQ (Frequently Asked Questions)"online: Robert Graham <http://www.robertgraham.com/pubs/carnivore-faq.html>, (date accessed: 28 December 2001).

10 Following the attacks on the United States 11 September 2001, voices of dissent have grown quieter.

11 In addition to the FBI site on Carnivore http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm, authoritative resources include S.P. Smith et al., *Independent Review of the Carnivore System – Final Report*, Illinois Institute of Technology Research Institute (8 December 2000) , online: US Department of Justice: <http://www.usdoj.gov/jmd/publications/carniv_final.pdf> (date accessed: 26 December 2002) and the Electronic Privacy Information Center http://www.epic.org/privacy/carnivore/.

12 For example, "John Schwartz, "Armey to Press Opposition to Net Wiretaps" *The New York Times*, June 14, 2001 Section C; Page 10; Column 6.

13 B.N. Meeks, "FBI's Carnivore Hunts in a Pack" *MSNBC* (17 October 2000), online: MSNBC http://znet.com.com/2100-11-524795.htm (date accessed: 24 December 2002).

14 J. Tyson, "How Carnivore Works" Marshall Brain's How Stuff Works 2001 online: How Stuff Works http://www.howstuffworks.com/carnivore.htm (date accessed: 19 December 2002).

15 Meeks, supra note 13.

16 Meeks, supra note 13.

17 I. Hands, "Carnivore – A Brief History & Synopsis"11 BlackBox 2001, online: Black Box http://black.box.sk/articles/11/carnivore.txt (date accessed: 29 December 2002).

18 Ibid.

19 Ibid.

20 Meeks, supra note 13.

21 Hands, supra note 17.

22 Ibid.

23 Meeks, supra note 13.

24 USA., Federal Bureau of Investigation, Phiple Troenix, 21 September 1998, online: EPIC <http://www.epic.org/privacy/carnivore/phipletroenix.html> (date accessed: 20 December 2002) [hereinafter "Phiple Troenix"].

25 Ibid.

26 Meeks, supra note 13.

27 Tyson, supra note 14.

28 Meeks, supra note 13.

29 Meeks, supra note 13.

30 Hands, supra note 17.

31 Ibid.

32 USA., Federal Bureau of Investigation, Carnivore Evolution, online: EPIC <http://www.epic.org/privacy/carnivore/evolution.html> (date accessed: 2 January 2002).

33 Meeks, supra note 13.

34 B. Sullivan, "FBI Software Cracks Encryption Wall" MSNBC (20 November 2001), online: MSNBC <http://www.msnbc.com/news/660096.asp> (date accessed: 26 December 2002).

35 Ibid.

36 Sullivan, supra note 34

37 "Fbi Confirms 'magic Lantern' Is Being Lit" National Journal's Technology Daily December 13, 2001

38 Sullivan, supra note 34.

39 Ibid.

40.In the "Guide to the Report to Congress" at http://www.darpa.mil/body/tia/terrorism_info_aware.htm (accessed 22 May 2003), DARPA suggests that the original name gave the impression that the TIA was to be used to develop dossiers on US citizens, rather than its real purpose better reflected in the new name.

41 JOHN MARKOFF and JOHN SCHWARTZ "Many Tools of Big Brother Are Up and Running" *The New York Times* December 23, 2002, Section C; Page 1; Column 2.

42 "DCS1000: The Device Formerly Known as Carnivore" Refuse & Resist (14 February 2001), online: Refuse & Resist! <http://www.refuseandresist.org/resist_this/021601carnivore.html> (date accessed: 27 December 2001) [hereinafter "DCS1000"].

43 E. Luening, "Don't be fooled: DCS1000 still a 'Carnivore' at heart"*ZDNet News* (9 February 2001), online: ZD Net <http://www.zdnet.com/zdnn/stories/news/0,4586,2684186,00.html>, (date accessed: 28 December 2001).

44 DCS1000, supra note 42.

45 Carnivore Diagnostic Tool, supra note 5.

46 Internet and Data, supra note 8.

47 Ibid.

48 Ibid. See also, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 USC. §§ 2510 - 2522

49 Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 USC. §§ 2510–2522

50 Internet and Data, supra note 8.

51 Ibid.

52 Ibid.

53 USA., Centre for Democracy and Technology, *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age*,(Testimony of James X. Dempsey before the United States Senate - Senate Judiciary Committee) (6 September 2000), online: Centre for Democracy and Technology <http://www.cdt.org/testimony/000906dempsey.shtml> (date accessed: 25 December 2002) [hereinafter "Carnivore Controversy"].

54 Internet and Data, supra note 8.

55 Ibid.

56 Ibid.

57 E. Murray, "FBI's Carnivore Probably Can't Shut Down Internet"25 July 2000, online: Eric Murray <http://www.lne.com/ericm/papers/carnivore.html> (date accessed: 26 December 2002).

58 Robert X Cringely "Meet Eater: The FBI's Plan for Digital Wiretaps Raises More Questions Than It Answers *PBS Pulpit* 13 July 2000 http://www.pbs.org/cringely/pulpit/pulpit20000713.html (date accessed: 26 December 2002).

59 S.P. Smith et al., *Independent Review of the Carnivore System – Final Report*, Illinois Institute of Technology Research Institute (8 December 2000) online: US Department of Justice: <http://www.usdoj.gov/jmd/publications/carniv_final.pdf> (date accessed: 26 December 2002).

60 Graham, supra note 9.

61 Ibid.

62 Michelle Delio "Snooping Isn't Email Delay Cause" *Wired News*, 25 September 2001, http://www.wired.com/news/culture/0,1284,47092,00.html

63 Although it is likely that systems like Echelon, discussed below, are occasionally employed in this way.

64 Graham, supra note 9.

65 Ibid.

66 Omnibus Crime Control and Safe Streets Act of 1968 (Title

III) 18 USC. §2518(5).

67 However, this was the software of choice for the Royal Canadian Mounted Police (RCMP) in their investigations of the MafiaBoy denial of service attacks. In conversations with officers at the 'In Search of Security" conference in Montreal in 2003, it would seem that Carnivore was not used in this investigation in Canada (though of course it may have been used in the US side of the inquiry).

68 T.C. Greene, "Carnivore substitute keeps Feds honest" *The Register*(2 October2001), online: The Register <http://www.theregister.co.uk/content/6/21992.html> (date accessed: 28 December 2001).

69 A. Harrison, "Security Software Vendor Develops Carnivore Alternative" *ComputerWorld* (21 September 2000), online: Computer World. <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO50930,00.html> (date accessed: 29 December 2001).

70 Ibid.

71 J. Lyman, "SilentRunner Spyware Out-Snoops FBI's Carnivore" *NewsFactor Network*(2 March, 2001), online: News Factor <http://www.newsfactor.com/perl/printer/7873/> (date accessed: 25 December 2001).

72 See SilentRunner details at www.silentrunner.com. (date accessed: 26 December 2002)

73 "NetWitness Analysis System" *Forensics Explorers* (2000), online: http://www.forensicsexplorer.com/ (date accessed: 26 December 2002) [hereinafter "Net Witness"].

74 Ibid.

75 Pen register refers to discovering the origin address of a communication.

76 Trap-and-trace is restricted to discovering the destination of a communication.

77 Ibid.

78 "WildPackets' EtherPeek, Ethernet Protocol Analyzer & Packet Debugger"(2000), online: <http://www.wildpackets.com/elements/EtherPeek.pdf> (date accessed: 14 June 2002) [hereinafter "WildPackets"].

79 Ibid.

80 Ibid.

81 "Hackers take to the air" BBC News (17 October 2001), online: BBC News <http://news.bbc.co.uk/hi/english/sci/tech/newsid_1596000/1596033.stm> (date accessed: 7 June 2002).

82 Ibid.

83 Scott Fluhrer, Itskik Mantin and Adi Shamir "Weaknesses in the Key Scheduling Algorithm of RC4" http://www.wisdom.weizmann.ac.il/mathusers/itsik/RC4/Papers/Rc4_ksa.ps.

84 "Air Snort", online: Personal Telco Project www.personaltelco.net/index.cgi/AirSnort (date accessed: 7 June 2002) [hereinafter "Air Snort"] and http://airsnort.shmoo.com (date accessed: 7 June 2002). See also "WEPcrack", online: Source Forge http://sourceforge.net/projects/wepcrack (date accessed: 7 June 2002).

85 Air Snort, supra note 83.

86 Ibid.

87 Tyson, supra note 14.

88 Ibid.

89 Jennings, supra note 7.

90 Ibid.

91 Ibid.

92 "How Does Carnivore Work?"About.com, online: About.com

http://email.about.com/library/weekly/aa102901a.htm (date accessed: 25 December 2001).

93 Smith, supra note 59.

94 Ibid.

95 All information regarding Carnivore's Filtering Modes was taken from : Smith, supra note 59.

96 Internet and Data, supra note 8.

97 R.F. Forno, "Who's Afraid of Carnivore? Not Me!" *InfoWarrior* (2 August 2000) , InfoWarrior <http://www.infowarrior.org/articles/carnivore.html> (date accessed: 24 September 2001).

98 Graham, supra note 9.

99 Ibid.

100 Ibid. Examples of anonymous remailers include Mixmaster http://sourceforge.net/projects/mixmaster/ (date accessed: 26 December 2002) and Private Idaho http://www.eskimo.com/~joelm/pi.html (date accessed: 26 December 2002).

101 Ibid.

102 Ibid.

103 For example, Deluxe Transitive Generatorhttp://www.anotherlongsleeplessnight.com/projects/deluxe.html (date accessed: 26 December 2002) automatically produces text such as "A halfhearted guardian angel befriends the starlet. A bubble living with the gonad is friendly. An ungodly tea party shares a shower with the alchemist around a tea party, but a likeable clodhopper avoids contact with a nefarious dissident."

104 Ibid.

105 Forno, supra note 97.

106 Graham, supra note 9.

107 Ibid.

108 Respectively at www.freedom.net, www.messagerx.com, and www.mail2web.com (date accessed: 26 December 2002).

109 See "Stop Carnivore NOW!" website online: <http://www.stopcarnivore.org> (date accessed: 29 December 2001) [hereinafter "Stop Carnivore Now"].

110 Earthlink http://www.earthlink.net/ fought a Carnivore order, lost, but then had the equipment removed after claiming that it interfered with the operation of their services; see http://www.stopcarnivore.org/carnfreeisps.htm (date accessed: 26 December 2002).

111 C. Oakes, "Will Crypto Feast on Carnivore? "*Wired News* (4 August 4 2000), online: Wired News <http://www.wired.com/news/print/0,1294,37915,00.html> (date accessed: 26 December 2002).

112 Smith, supra note 59.

113 Ibid.

114 Graham, supra note 9.