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 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]

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

> *[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

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.

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

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 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]

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

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 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.

Going for the throat: Carnivore in an ECHELON world - Part II

Talitha Nabbali, Graduate 2002, University of Western Ontario &
Mark Perry,[1] 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, provides an overview of the FBI's Carnivore electronic surveillance system.

A. Carnivore and American law

There are many laws in the United States that make pen-register, trap-and-trace and wiretap surveillance legal. Yet, none of these laws specifically address electronic surveillance using IP sniffers such as Carnivore. Nonetheless, the FBI and the government maintain that the laws allowing for telephone surveillance can be applied to Carnivore and other such surveillance devices. The FBI and the US government maintain that Internet surveillance is analogous to telephone surveillance for which most of the laws concerning wiretapping were formulated.

The analogy between the telephone and the Internet is important in regards to the different set of laws applicable to Carnivore's two operating modes; pen mode and full content mode. The difference between Carnivore's two modes of operation is that pen mode allows the FBI to intercept origin and destination information (the envelope of the e-mail) as well as URLs of sites visited, whereas full-content mode allows the FBI to collect substantive data in addition to transactional information. By using the telephone analogy the FBI claims that they need not demonstrate probable cause when using Carnivore in pen-mode, since Carnivore should be subject to the same minimal legal restraints as pen registers used to record a telephone subscriber's outgoing calls and trap-and-trace devices that record incoming telephone numbers for a particular subscriber.[2] Meanwhile, as with wiretaps on telephones, the FBI agrees that a higher legal threshold is needed to obtain a warrant for use of Carnivore in full-content mode.

This section will provide an overview of the laws that allow for Carnivore given that we accept that the Internet is sufficiently analogous to the telephone system for the purposes of wiretapping and investigation laws.[3]

The Omnibus Crime Control and Safe Streets Act governs the electronic interception of wire and oral communications. It places a higher burden on real time interceptions of oral, wire and electronic communications than the Fourth Amendment requires.[4] In accordance with this Act, only judges can authorize applications for wiretaps. In order to obtain an authorization for a wiretap, law enforcement officials must demonstrate probable cause that a crime has been committed or is about to be committed, that normal investigative procedures have been tried and have not been sufficient and that the intercepted communications will most probably be relevant to the investigation.[5]

Title III mandates that a wiretap order must contain:[6]

- The identity of the person to be surveyed;
- The nature of the communications to be intercepted;
- The location of the facility where the court order to intercept is granted;
- A description of the type of communications to be intercepted;
- A statement of the particular offense to which these communications relate;
- The identity of the law enforcement agency authorized to intercept the communications;
- The period of time for which the interception is authorized;
- Whether the surveillance will be terminated as soon as communications related to the offense are obtained

In addition, Title III states that the interception of communications must be minimized, such that no additional communications other than those that the court order allows shall be captured or recorded.[7] For example, in the case of telephone surveillance, if the child of a suspect calls a friend, surveillance must be terminated for the call.[8] Not only can the call of the child not be recorded, but law enforcement agents are not even allowed to listen to the call. Title III also demands, that within 90 days of the termination of the investigation, all targets and other parties whose communications were captured are notified of interception.[9]

Although, Title III of the Omnibus Crime Control and Safe Streets Act mandates that a court order must be awarded before any surveillance is to take place, there are exceptions, namely in cases where national security is compromised or there is an immediate danger of death or serious injury. However, even in such cases, interception can only proceed if a court order is given within 48 hours of the start of surveillance.[10]

Even though Title III imposes many regulations for full wiretaps, the restrictions on pen registers and trap-and-trace devices are far less stringent. Law enforcement agencies are not required to demonstrate probable cause when using either a pen register or a trap-and-trace device[11] since in accordance with Title III the use of either pen registers or trap-and-trace devices does not constitute a search under the Fourth Amendment.[12]

The Electronic Communications Privacy Act amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to create statutory legal protection for all types of wire and electronic communications content, including, but not limited to, computer and Internet based communications.[13] Furthermore, ECPA clarified the difference between the obtainment of wiretap orders and pen-register and trap-and-trace orders by declaring that to wiretap communications “an agency must obtain a warrant based upon probable cause”, but to obtain a pen-trap order “an agent must merely certify that the information likely to be obtained is relevant to an ongoing criminal investigation.”[14]

The rationale behind the difference in obtaining these court orders is that, according to the Supreme Court of the United States’ 1979 decision in **Smith**[15] there is no expectation of privacy in telephone numbers dialed in and numbers received.[16] Therefore transactional information (addressing, routing, billing and other information generated by service providers) is not to be awarded the same level of protection as substantive data.

The Communications Assistance for Law Enforcement Agencies Act 1994 (CALEA)[17] requires phone companies to possess the infrastructure to support surveillance tools such as pen register and trap-and-trace devices. More specifically, CALEA requires that all companies providing telecommunication services to the US install remote control ports on their routes that allow law enforcement agencies to easily extract any conversation in its entirety, up to 1% of the hub’s total traffic simultaneously.[18] The installation of the remote control ports was to be done by 1998, unless a waver was issued to extend implementation to October 24, 2000.

The FBI sometimes names CALEA as proof that their use of Carnivore is legal. Yet, the United States Court of Appeals for the District of Columbia Circuit noted in **United States Telecom Association**[19] that “Because Congress intended CALEA to "preserve the status quo," the Act does not alter the existing legal framework for obtaining wiretap and pen register authorization”, "providing law enforcement no more and no less access to information than it had in the past.". CALEA does not cover "information services" such as e-mail and internet access.”[20]

The FBI sometimes names CALEA as proof that their use of Carnivore is legal

The 21st Century Department of Justice Appropriations Act[21] passed in the House of Representatives on July 23, 2000, requires the FBI to provide an annual report to Congress detailing exactly how, when, where and why Carnivore has been deployed during the previous year. The Act was passed because Congress recognized that the FBI’s Carnivore surveillance system posed a potential threat to individual privacy.[22] Section 306 of the Act demands that the annual report provided by the FBI detail:

- The number of times Carnivore has been deployed;
- The officials who approved of each use;
- The criteria used to approve the deployment request;
- The process used to submit, review and approve the request;
- The facilities where Carnivore boxes were placed;
- The information gathered during each deployment.

Both the Combating Terrorism Act of 2001 and the USA Patriot Act of 2001 were approved by the Senate in the wake of the terrorism attacks of September 11, 2001.[23] Both Acts enhance police wiretapping to more situations and make it easier for the FBI to deploy Carnivore.[24] With the implementation of these acts, any US or State

Attorney General can give a court order for the installation of a Carnivore box, whereas previously only a judge could order such warrants.[25] Although it is possible to get a court order allowing for the interception of Internet transmissions from a US or State Attorney General, surveillance with such orders are limited to pen-mode collection.[26] In order to intercept substantive data the FBI must still seek a court order from a judge. The Combating Terrorism Act and the USA Patriot Act also extend circumstances where interception can begin without a court order to include "safety or attacks on the integrity or availability of a protected computer", making computer hacking offenses comparable to threats to national security, public health and crimes that cause death and serious injury.[27]

B. Other electronic surveillance

In order to make surveillance easier and to provide a salve to public unease concerning criminal activity on the Internet, many countries have passed legislation to make surveillance easier and more comprehensive. Most of these newly established legislations attempt to extend the interception capabilities that law enforcement agencies have over telephone communications (circuit switched networks) to Internet communications (packet switched networks), and make interesting comparisons to the US approach with Carnivore and supporting legislation. Following is an overview of the laws and policies regarding electronic surveillance around the world.

The United Kingdom's Regulation of Investigatory Powers Act 2000 (RIPA), which received royal ascent on July 28, 2000,[28] is one of the most controversial surveillance laws in the world. RIPA has been deemed "the most pernicious invasion of privacy ever imposed by a modern democratic state",[29] and has been criticized as violating the European Convention on Human Rights. The Act is composed of five parts, which include provisions for listening to mobile and satellite phone calls, intercepting pager messages and bugging switchboards.[30] However, the most controversial provisions are those concerning Internet surveillance. The legislative act forces all ISPs in the United Kingdom to install black boxes on their network to monitor all data as it passes and subsequently feed it to a central processing location controlled by the United Kingdom's security service MI-5. Moreover, the Act contains provisions for government access to encryption keys ("GAK").

The RIPA applies to "any system which exists (wholly or partly) in the United Kingdom".[31] Thus, everything sent to or through Britain is subject to surveillance, under the law. Considering the nature of Internet packet routing, this means that any packet could travel through Britain's communication infrastructure and thus be surveyed by British intelligence. In order for surveillance of all Internet traffic to be possible, RIPA compels ISPs to install 'black boxes' that, when activated, send intercepted communications directly to MI-5's new central monitoring station, the Government Technical Assistance Centre (GTAC) located inside MI-5's London Headquarters. Controversially, RIPA specifies that requests for traffic data, e.g. web sites accessed, intended recipients of sent and received e-mails and logon transactions, do not require a warrant because such information is "purely statistical"[32] and therefore can be requested by any governmental department in the interest of detecting crime.[33] In other words, RIPA allows for the mass surveillance of internet activities without judicial warrant or adequate oversight. Consequently, the act increases the power of public authorities without correspondingly increasing the scope of their oversight or their accountability.[34]

However, like in American Law, under RIPA the content of communications can only be intercepted with a court order, although the reasons for a warrant are broad:[35]

> *(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary--*
>
> *(a) in the interests of national security;*
>
> *(b) for the purpose of preventing or detecting serious crime;*
>
> *(c) for the purpose of safeguarding the economic well-being of the United Kingdom; or*
>
> *(d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.*

Although RIPA demands that a court order for interception be obtained, it makes it a criminal offense to reveal to anyone that they are being surveyed or have been surveyed. According to RIPA, the revelation of the content, details or the existence of a surveillance warrant past or present bears a penalty of up to five years in jail.[36] Consequently, because the existence of surveillance warrants are to be kept secret indefinitely, the British public will never be aware of the scope of MI-5's electronic surveillance.[37]

Although the power granted by the Regulatory Investigatory Powers Act of 2000 to law enforcement officials in regards to electronic surveillance is very broad, it is the fact that RIPA contains provisions for government access to encryption keys (GAK) that has generated the most controversy. With the royal ascent of RIPA, the UK joins Malaysia, Singapore and India as the only countries in the world to pass key seizure legislation.[38] Under RIPA, encryption keys of individuals, users and companies can be warranted for the purpose of any type of investigation for which a warrant would be issued.[39] Lack of cooperation in regards to the handing over of encryption keys can result in a prison sentence of two years. Furthermore, as with warrants to intercept communications content, there is a silence imposed on the recipient of an encryption key disclosure order. However, it is questionable whether RIPA's GAK provision will be effective to deter crime. After all, criminals who are careful and clever in their use of computers and the Internet are capable of avoiding surveillance,[40] while criminals who are caught and forced to hand over their cryptographic keys would rather claim they lost their key and endure a maximum of two years in prison than hand over a key which could produce damning evidence of more heinous crimes.[41]

Opponents of RIPA allege that the Act's GAK provision breaches the European Convention on Human Rights Act 1998, which demands that legislation within all countries of the European Union meet several requirements, such as respect for private life and the right to a fair trial.[42] The argument is made that under RIPA the right to a fair trial is impossible since the Act demands that Internet users provide encryption keys on pain of imprisonment, that is, the Act forces Internet users to incriminate themselves.[43] As there is a general right against self-incrimination, which forbids government officials from compelling a person to testify against herself, RIPA contravenes basic human rights. RIPA also breaches article 6 of the Human Rights Act of 1998, which states that the burden of proof cannot be reversed such that a suspect needs to provide the requested evidence to prove his innocence,[44] since RIPA puts the onus on Internet users to prove that they do not have a requested key or they have lost it.[45] Given its problems with human rights, RIPA would without a doubt be deemed unlawful if the United Kingdom legislation was subject to such restraints.[46] RIPA cannot be revoked by a legal decision in the UK as constitutional challenges of this nature are not possible. Nonetheless, it is expected that RIPA will be challenged in the European Court of Human Rights.

Not only is RIPA's violation of human rights disconcerting, but its negative economic impact on the United Kingdom is also alarming. According to a report commission by the British Chambers of Commerce on the Bill, RIPA's:

> *effect is likely to be a loss of confidence in e-commerce, unacceptable costs to business, and to the UK economy, confusion and uncertainty at numerous levels of business and an onerous imposition of the rights of individuals.*[47]

The report claims that the cost of compliance to RIPA for British ISPs will be £640 million over the next five years and the loss and leakage to the UK economy will be about £46 billion in RIPA's first five years of implementation.[48] Furthermore, RIPA's key seizure provision creates many business risks including increased opportunity for industrial espionage, reduced trust and confidence in company security and market disadvantage in the global marketplace.[49] Many believe that investors and e-commerce will only return to the United Kingdom, when all countries impose such oppressive restrictions on Internet users.[50]

RIPA undermines the privacy and security of honest citizens

It can be argued that not only does RIPA seem to metamorphosis the United Kingdom from a modern democratic state into a surveillance nation, it also seems to hold potential problems for the economy, whose Labour government had aimed to make it the most e-friendly state in Europe by 2002.[51] Ironically, RIPA undermines the privacy and security of honest citizens and businesses, yet is most probably ineffective against criminals who are careful and sophisticated in their use of computers and the Internet.

On July 10, 2000, Ireland passed the Electronic Commerce Act of 2000[52] which the Irish government believes will help Ireland become a hub for e-commerce.[53] The Act guarantees that Internet users within Ireland shall enjoy high levels of privacy by making it an offense for anyone, including law enforcement officials, to attempt to access the content of encrypted communications without authorization.[54] Although the Act provides extensive protection for encrypted communications, it does not prevent law enforcement officials from intercepting unencrypted communications, which is allowed under Ireland's Interception of Telecommunications Act of 1993.[55]

Russia's Sisterna Operativno-Rozysknykh Meropriyatti, known in English as Russia's System of Operative Investigative Procedures or System of Ensuring Investigative Activity was introduced in two parts. The first part, SORM-1, came into affect in 1994 and gave the FSB, Russia's internal counterintelligence service (formerly known as the KGB), the right to monitor all telecommunications transmissions provided they first obtained a court order.[56] The second phase of the SORM legislation, SORM-2, came into affect in July 1998,[57] and requires that all ISPs install black boxes that provide a secure link between their ISP and the FSB's Data Collection Center (DCC)[58] such that the DCC can capture Internet transmissions within seconds.[59]

In many respects, SORM is very similar to the United Kingdom's Regulation of Investigatory Powers Act (RIPA) since both legislative acts allow for the widespread surveillance of Internet communications within their respective jurisdictions.[60] However, although the United Kingdom is considered far more democratic than Russia, it seems that the abolishment of SORM is more probable than the revoking of RIPA. SORM has never been passed in Russian Parliament and as it stands contravenes article 23 of the Russian Constitution, which guarantees a right to secrecy of communications.[61] Therefore, through legal challenges SORM can be revoked or altered.

Through Russia's democratic appellate process SORM has already been altered. In 2000, SORM was challenged in the Supreme Court of Russia by an appeal filed by a St. Petersburg journalist named Pavel Netupsky.[62] The result of this appeal was that the Supreme Court of Russia nullified article number 130 of the Ministry of Communications Order, which allowed the FSB to survey electronic communications without informing ISPs of the reason or the target of their surveillance.[63] After having abolished article 130 of the Ministry of Communications Order, electronic surveillance can now only be conducted if a court order, specifying the reasons for surveillance, is presented to an ISP.[64] It is important to note that although ISPs will know the identity of the person or persons being surveyed, this does not mean that the target of an investigation will be notified that they have been surveyed or are being surveyed. Therefore, although SORM has been altered, it still seems to contravene article 23 of the Russian Constitution. Consequently, it is evident that only through multiple legislative amendments will SORM possibly become constitutional. Nonetheless, following the crisis of Chechen guerrillas taking theatregoers hostage in October 2002, there were many reports of Russian cell phone users seeing that their encryption services were no longer functional, believed to be removed to allow for SORM wiretapping of cell communications.[65]

On August 13 1999, the Diet, the Japanese legislative assembly, passed the Communications Interception Law, modeled after the 1994 American Communications Assistance for Law Enforcement Agencies Act (CALEA), which allows law enforcement agencies to wiretap telephone, fax and internet communications.[66] It has been rumored that Japan was pressured into creating such a law by the United States government.[67] Prior to passing of the Communications Interception Law, wiretapping was illegal in Japan because it was said to violate article 21 of Japan's constitution and was explicitly prohibited under article 104 of Japan's Telecommunications Business Law and article 14 of Japan's Wire Telecommunications Law. [68]

The Japanese Wiretapping Act, which came into affect in August 2000, authorizes the use of wiretaps for cases involving drug trafficking, gun running, mass smuggling and gang-related murders.[69] The act requires that all ISPs make a pen-register style log of all Internet communications that can be subpoenaed at any time.[70] According to the law, prosecutors, senior police officers, narcotic controllers and officials of Japan's Maritime Safety Agency can apply for warrants to use wiretaps.[71] Because the Japanese are very concerned that the wiretapping law may be abused, warrants allowing for wiretaps can only be obtained from district court judges and are valid for a mere 10 days (but can be extended for up to 30 days).[72] Furthermore, the legislation makes it obligatory for an independent third party, such as an employee of Japan's Nippon Telegraph and Telephone Company, to monitor the wiretap.[73] The act also makes it mandatory that individuals who have been monitored are notified within 30 days of the end of the investigation[74] and prevents law enforcement agencies from wiretapping the communications of lawyers, doctors and religious leaders.[75]

Little information is known about the Royal Canadian Mounted Police's (RCMP) use of electronic surveillance since the RCMP refuses to publicly acknowledge whether they have electronic surveillance capabilities.[76] However, many believe that the RCMP is using the FBI's Carnivore surveillance system to intercept the electronic communications of suspected criminals.[77] As the RCMP regularly works closely with the FBI on matters of mutual interest, it is certainly likely that the RCMP would take advantage of the Carnivore program to combat online criminal activity. However, the FBI claims that the Carnivore program has never been used outside the United States.[78] Yet, the FBI does admit that they would allow the RCMP to use the program if the need arose.[79]

Although the FBI denies that Carnivore has been used by the RCMP, this does not mean that the RCMP is incapable of electronic surveillance. It is a known fact that the Canadian Security Establishment (CSE), a participant in ECHELON, conducts electronic surveillance. Thus the RCMP could work in conjunction with the CSE to intercept Internet communications. No matter the technology that the RCMP uses to conduct electronic surveillance, it is likely that they are capable of surveying Internet transmissions. Without a doubt information related to the RCMP's electronic surveillance capabilities will become available as surveillance of the Internet becomes widespread and intercepted electronic communications are used as evidence in Canadian courts.

On June 7 2000, the Australian government passed the Telecommunications Legislation Amendment Bill 2000 or TILAB 2000. The Bill creates two new types of warrants for electronic communication surveillance. The first, known as a "Named Person Warrant" allows law enforcement agencies to request permission to track a person's Internet activity without having to identify why or by which means they will monitor the person. The second is a special type of warrant called a "Foreign Communications Warrant" which permits law enforcement agencies to intercept electronic communications crossing Australia's border "for the purposes of collecting foreign intelligence."[80]

C. Carnivore controversy

As soon as the FBI announced they developed the Carnivore electronic surveillance system critics deemed the system unlawful. Opponents of Carnivore allege that the surveillance system invades privacy, limits liberty and violates the Fourth Amendment of the US Constitution. Organizations such as StopCarnivoreNOW!, the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) have petitioned the American government to stop deployment of Carnivore.

Although the American government heard the cries of outrage regarding Carnivore, very little was done to appease the critics or address their concerns. The only initiative taken by the US Government to calm Carnivore's opponents was to commission an independent review of the Carnivore electronic surveillance system.[81] Instead of shedding light on the constitutionality, the functionality and the FBI's usage of the system, the review did nothing more than enrage critics who deemed the review biased and hamstrung.

The FBI claims that use of Carnivore is permissible since electronic surveillance conducted by Carnivore is analogous to the wiretapping of telephone systems. In other words, the FBI claims that usage of Carnivore is in accordance with pre-existing laws regarding surveillance, namely Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communication Protection Act of 1986. The use of Carnivore in full-content mode is analogous to a wiretap of a telephone call, and consequently the same laws that apply to wiretaps should apply to Carnivore when it is operating in full-content mode. However, questions remain regarding whether the analogy between the operations of Carnivore in pen-mode and the operations of pen registers and trap-and-trace devices used on the telephone system is accurate.

The FBI claims that use of Carnivore is permissible since electronic surveillance is analogous to the wiretapping of telephone systems

Critics claim that use of Carnivore in pen-mode allows the FBI to access a much larger scope of data than traditional pen-registers and trap-and-trace devices used on phone systems.[82] First, Carnivore boxes are installed on an ISP's data network and not a telephone line, therefore information collected by Carnivore is not limited to the target's communications as it is when a pen-register or trap-and-trace device is used on a suspect's private telephone line.[83] Furthermore, in telephone systems with digital switching technologies, out-of-band signaling is used, meaning that call routing information (transactional information) is carried on a different channel than the conversation itself (substantive information). In older analog telephone systems, transactional information and substantive data are carried on the same channel, but the signaling of transactional information, the information collected by pen-register and trap-and-trace devices, consists of pulses and tones whereas the conversation is encoded differently. Therefore, in both digital and analog telephone systems it is impossible to capture substantive information using either pen register or trap-and-trace devices.[84] However, when transmitting data over the Internet, with the exception of FTP (File Transfer Protocol) data, both transactional information and substantive information are combined in the form of packets, making addressing information impossible to separate from content data.[85] Furthermore, since both Internet transactional and substantive data are recorded in digital form, any machine or system that can process one can process the other, such that it is impossible to be certain that the processing of transactional information does not intentionally or unintentionally divulge content data.[86]

Moreover, traditional pen-register and trap-and-trace devices only collect telephone numbers. However, when Carnivore is used in pen-mode it collects the subject line and content of e-mails, replacing each character of these fields with an "X".[87] Therefore, through use of Carnivore the FBI can record the length of each data field of an electronic communication.[88] Although the length of telephone calls are legally recordable, there is nothing in the laws related to phone tapping that can be analogous to recording the length of individual data fields, as is the case with Carnivore.[89] The fact that Carnivore documents the length of individual fields might seem insignificant, yet much can be deduced from such information. For instance, take the case of a child pornography suspect, the FBI surveys his communications in pen-mode and notices that although most of his messages are small, some are extremely large, indicating that perhaps illegal pictures are being transferred. The FBI can then take the destination information of these large files and start surveying the recipients of these files as to discover a potential child pornography ring.[90] Although clearly arguable that such measures are a 'good thing', such surveillance is illegal, since developing additional leads or charges against a suspect in this fashion is impermissible without following the correct procedure for a full investigation.

In addition, e-mail addresses and URLs reveal much more information than do digits in telephone numbers.[91] Telephone numbers only reveal the location from where a call is placed and the person to whom the number is registered.[92] In contrast, e-mail addresses can reveal the identity of corresponding parties, an individual's organizational affiliations and perhaps even personal characteristics.[93] For instance, take one of the authors' email addresses, markperry@acm.org, markperry@mac.com and mperry@uwo.ca - revealing affiliation with the Association of Computing Machinery, which the author uses an Apple computer and is also associated in some manner with the University of Western Ontario.

Lastly, even if use of Carnivore in pen-mode is deemed lawful, the fact that ISPs have no control over Carnivore's deployment is inconsistent with pre-existing laws.[94] The FBI retains the sole right to alter a Carnivore box's operation once it is in place. Furthermore, the FBI can do so remotely without the knowledge or the cooperation of the ISP.[95] If Carnivore's surveillance is analogous to telephone surveillance, than why is such surveillance not conducted similarly? In the world of telephone surveillance, telephone utility companies have been extremely reluctant to allow law enforcement agencies into their switching facilities in order to survey their customers.[96] Instead, telephone companies themselves have satisfied court orders and subsequently passed on subpoenaed information to law enforcement agents. Why are the same protocols not applied to ISPs in the case of Internet surveillance? After all, ISPs best understand their own network and are in the best position to lawfully comply with a court order since they have a dual duty to produce subpoenaed information and to protect their customers' interest.

It seems that for the FBI to rationalize the use of Carnivore they must implement laws specific to Internet surveillance, since the analogy between the telephone system and the Internet is too weak to uphold Carnivore's surveillance as legitimate.[97] When asked if existing laws protecting the privacy of telephone communications are enough to protect e-mail and online activities in April 2001, 62% of the survey responded that new laws need to be written to protect online privacy.[98] However, in September 2002, the same pollster reports:[99]

> *[C]itizens are sharply divided on the question of whether the government should be able to monitor people's email and online activities. The opinion breakdown on the question is 47% of Americans believe the government should not have the right to monitor people's Internet use and 45% say the government should have that right. A majority of Internet users oppose government monitoring of people's email and Web activities.*

There has been discussion regarding whether or not the Carnivore electronic surveillance system violates the Fourth Amendment of the US Constitution. Opponents of Carnivore have deemed the system comparable to "a super wiretap capable of listening to all calls placed by all customers of a telephone company".[100] Critics claim that Carnivore contravenes the literal interpretation, in addition to the figurative interpretation of the Fourth Amendment. According to them, Carnivore violates the condition that a warrant must particularly describe the "place to be searched and the persons or things to be seized" given the nature of the Internet does not allow the "place to be searched" to be "particularly described".[101] For instance, take a targeted suspect surfing a site in California, the FBI gets a court order to intercept the Internet communications of the suspect on his ISP's network in New York, how could the court order include the interception of his surfing activity hosted on the Californian site?[102]

Critics also condemn Carnivore, stating that its usage by the FBI contravenes the Fourth Amendment's reasonable expectation of privacy because it over collects information while being used in pen-mode. According to critics of the system, Carnivore has the potential for misuse since the software can be improperly calibrated by pushing the wrong set of radio buttons allowing the interception of more information than is subpoenaed.[103] Even, the Independent Review of the Carnivore surveillance system claims that this problem should be addressed without further delay by creating two different versions of the Carnivore system, one for pen-mode operations and the other for full-content interceptions.[104]

However many critics believed that even if two distinct Carnivore systems were created, Carnivore would still violate the Fourth Amendment. They argue that people seek the benefits of anonymity when using the Internet,[105] for instance in chat rooms, where they are not susceptible to approval or contempt from third parties[106] and online shopping where they do not have to reveal their personal preferences, for example their waist size or their tastes in music or books.[107] With the use of Carnivore lurking on the Internet, Internet users will lose their anonymity and will begin to behave differently online.[108]

In the eyes of Carnivore's opponents, the Fourth Amendment, which was created in order to "protect the rights of Americans while they work and play on the Internet as it does in the physical world",[109] is violated by Carnivore. Given the fact that "Americans use the Internet everyday to transfer vast amounts of private data, financial statement, medical records, e-mail, online reading and shopping habits, business transactions and Web surfing"[110] they have the right to know that their personal information is being transmitted safely, without being copied by government investigators, since the amount of sensitive information being transmitted over the Internet is enough to allow the Government to form a "granular picture of their (an internet user) interests and activities"[111] and to allow the government to develop suspicions against them. Opponents of Carnivore maintain that if the US Government does not respect its citizens' right to privacy nothing remains to keep American society liberal and democratic.

The Independent Technical Review of the Carnivore System commissioned by the Department of Justice and undertaken by the Illinois Institute of Technology[112] has been subject to much criticism. Many have deemed the report biased and inadequate.

The Independent Technical Review of the Carnivore System has been subject to much criticism

The American Civil Liberties Union (ACLU), amongst others, has "expressed substantial reservations about both the independence of the reviewers and the proposed scope of their review."[113] They claim that for the review to be truly independent it would need to be external to the Department of Justice (DoJ), which it was not since the review was overseen by the government officials who employ Carnivore (FBI & the DoJ). Furthermore, the ACLU claims that the government chosen review panel was constrained since the review team consisted of former governmental advisors, a former Clinton information policy advisor, former DoJ officials and others with backgrounds in the National Security Agency (NSA) and the Department of Treasury. The ACLU also asserts that a single one-time review of Carnivore is inadequate since Carnivore will be replaced with its progenitors and the only way to ensure full compliance of all future versions of Carnivore would be continual oversight of the system.[114] Critics of the IITRI report also believe that the government placed unreasonable restrictions on the review panel, including limits on the information available to the reviewers and specifications for the review that are dictatorial.[115] Consequently, critics question the conclusions of the review. According to them, even if the review was conducted in good faith, to the best of IITRI's ability, the limitations imposed on IITRI and the financial and time constraints placed on the review cannot support a conclusion that Carnivore is correct, safe and always consistent with American Law. One report notes:[116]

> *Although the IITRI study appears to represent a good-faith effort at independent review, the limited nature of the analysis described in the draft report simply cannot support a conclusion that Carnivore is correct, safe, or always consistent*

with legal limitations. Those who are concerned that the system produces correct evidence, represents no threat to the networks on which it is installed, or complies with the scope of court orders should not take much comfort from the analysis described in the report or its conclusions.

Furthermore, the fact that the Department of Justice bestowed a “daunting list of requirement and restrictions for the review”, and retained final authority over the report drove numerous university research teams to forego the opportunity to review the Carnivore system citing that such strict control by the DoJ would prevent an independent review of the system.[117] Among the universities that declined requests to review the Carnivore electronic surveillance system were the Massachusetts’s Institute of Technology (MIT), the University of California at San Diego, Dartmouth College, the University of Michigan and Purdue University.[118]

D. ECHELON

No discussion of electronic surveillance would be complete without a description of ECHELON, the term popularly used for an automated global interception and relay system, said to carry out “quasi-total surveillance” of all communications.[119] It must be made clear that ECHELON and similar systems are outside the normal operations of law enforcement envisaged when implementing Carnivore, or surveillance under RIPA. ECHELON is ‘1984’ now, with little oversight by government or community.[120] The system is operated by intelligence agencies in the United States, the United Kingdom, Canada, New Zealand and Australia.[121] The ECHELON system is primarily used and designed to intercept the Internet, fax and telephone communications of non-military targets,[122] specifically communications relating to terrorism, organized crime, economic dealings and scientific developments.[123] It is rumored that the system collects as many as 3 billion communications a day,[124] and sifts through 90% of all Internet traffic.[125] Although ECHELON is the only documented global interception system, it is likely that other nations such as France and Russia also survey international communications.

It is important to note, that ECHELON, unlike Carnivore, is not designed to eavesdrop on a particular individual’s communications. Instead, the system works by indiscriminately intercepting very large quantities of communications and then distills the collected data through artificial intelligence programs to extract messages of interest from the mass of unwanted ones.[126] The ECHELON system is composed of a chain of interception facilities located around the world that tap into all the major components of international telecommunications networks, including international telecommunications satellites (Intelsat), regional communication satellites, radio communications, and land-based communication networks (microwave and cable).[127] These globally positioned facilities are linked together such that the data they intercept is available to the other states participating in ECHELON.[128] The United States’ National Security Agency (NSA) is by far the senior partner participating in ECHELON, the agency employs over 21 000 people and has a budget of over US $3.6 billion, a larger operating budget then either the FBI or the CIA.[129] The other partners; the Government Communications Headquarters (GCHQ) in the United Kingdom, the Communications Security Establishment of Canada (CSE) (which employs 890 people and has an operating budget of CAN $110 million), the Defense Signals Directorate (DSD) in Australia and the Government Communications Security Bureau (GCSB) of New Zealand, share the cost of ECHELON’s operations with the NSA and make joint use of the resulting information.[130]

The alliance between these five nations grew from co-operations during World War II to intercept radio transmissions and was formalized in 1948 with the signing of the UKUSA signals intelligence agreement (SIGINT), which aimed primarily to monitor the activities of the USSR.[131] It wasn’t until 1971 that the UKUSA allies began ECHELON.[132] Before then, each ally did their intelligence gathering operations independently from one another.[133] Under ECHELON, the task of surveying the world’s communications is divided among the participating states. The United Kingdom has the task of surveying Africa and Europe up to the Ural Mountains of the former USSR, Canada has the task of surveying the northern latitudes and the Polar Regions, Australia and New Zealand survey Oceania and the areas surrounding the Indian Ocean, and the United States surveys North and South American transmissions as well as Pacific Intelsat transmissions.[134] Known surveillance stations are located in Yakima, Washington and Sugar Grove, West Virginia in the United States, Sebana Seca in Puerto Rico, Morwenstow and Menwith Hill in England, Geraldton, Pine Gap and Shoal Bay in Australia, Misawa in Japan, Waihopai in New Zealand, Leitrim, Ontario in Canada and Bad Aibling, Germany.[135]

At each of these respective stations, there is a computer known as an ECHELON "Dictionary".[136] Each ECHELON Dictionary is programmed daily with keywords that can be anything, including names of people, locations, ships, countries, organizations, telephone numbers, subject names and Internet addresses, or any other word of interest (e.g. "nitroglycerine") and intercepts messages containing these keywords. However, the Dictionary at each station, not only searches intercepted messages for words inputted by its parent agency, but also searches captured data for keywords entered in partner nations' Dictionaries.[137] Whenever a Dictionary discovers a message containing a keyword of another agency, it automatically picks up the message and sends it directly to the headquarters of the agency that inputted that specific keyword.[138]

ECHELON's participatory countries intercept communications in many ways. The most common methods of interception are massive ground radio antennas, interception satellites and IP sniffer devices[139] that are capable of handling much larger quantities of data than Carnivore boxes. However, ECHELON uses many other methods to intercept telecommunication transmissions. For instance, it is believed that American divers tap into cables carrying phone calls across the sea and install surveillance devices.[140] Furthermore, it is believed that the ECHELON network has buildings situated along microwave and cable routes to intercept communications,[141] and that other transmissions are captured from space using spy satellites. In addition, it has been said that ECHELON intercepts communications through "embassy collection": ECHELON's embassy collection program reputedly places sophisticated receivers and processors in diplomatic bags in overseas embassies, which are then used to monitor communications in foreign capitals.[142]

Although, information in regards to ECHELON does exist, the US and other participating governments have gone to extreme lengths to keep details of ECHELON operations secret. The US government takes this further, and still refuses to admit that ECHELON exists, even though both Australia and New Zealand have confirmed the system's existence.[143] As ECHELON's existence is confirmed, many privacy organizations and individuals are now concerned about whether ECHELON follows any legal standards. In an attempt to answer this question, the Electronic Privacy Information Center sued the US government, without success, hoping to obtain documents describing the legal standards by which ECHELON adheres, if any exist.[144] Unlike the Carnivore system, whose use must conform to US surveillance laws, ECHELON engages in a subterfuge to avoid legal restrictions, which many countries have in place to prevent invasions of privacy.[145] For instance, it is rumored that nations would not use their own agents to spy on their citizens, but instead would assign the task to the spy agency of one of the other allies participating in ECHELON.[146] Since the interception of communications taking place within a given country does not target the citizens of that country, a person whose messages are intercepted does not have any domestic legal protection.[147]

It seems that the only concern raised in regards to ECHELON, in the US in particular, is whether the interception system targets domestic traffic. Even when the US Congress held hearings concerning the activities of NSA, these hearings were confined to whether US citizens were affected by NSA's surveillance, without any real concern expressed regarding the legality of NSA's surveillance or the existence of the ECHELON surveillance system itself.[148] As evidence indicates that domestic traffic is not intercepted by internal spy agencies, ECHELON continues to exist with little resistance. However, it is likely that if a US agency required information on a US citizen it could ask one of the other ECHELON facilities to oblige in gathering information. The US facility would then not be spying on a US citizen, though the effect would be the same. This technique was reportedly used by Margaret Thatcher.[149]

It is unlikely that the FBI will stop using Carnivore

E. Conclusion

Although the FBI's Carnivore electronic surveillance system has been plagued with bad publicity and is in dire need of improvement in order to make it comply transparently with American laws regarding surveillance, it is unlikely that the FBI will stop using Carnivore. Without Carnivore or a comparable software suite, the FBI would be unable to conduct electronic surveillance. Consequently, it is evident that Carnivore is an asset to the FBI. However, the FBI seems unwilling to neither admit the shortcomings of the software nor allow that the software must be improved and its use must be subject to strict regulations such that it does not infringe upon the freedom and the right to privacy of American citizens. Currently the FBI maintains a viewpoint that public safety is by far the most important concern of Americans. Following the attack on the United States on 11

September 2001 they face much less opposition than before that time. However, John Ashcroft, the current Attorney General of the United States, who is not known for his liberal views remarked (in relation to encryption controls): [150]

> *There is a concern that the Internet could be used to commit crimes and that advanced encryption could disguise such activity. However, we do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant the government the Orwellian capability to listen at will and in real time to our communications across the Web? The protections of the Fourth Amendment are clear. The right to protection from unlawful searches is an indivisible American value. Two hundred years of court decisions have stood in defense of this fundamental right. The state's interest in effective crime-fighting should never vitiate the citizens' Bill of Rights.*[151]

The first step in order to make Carnivore an acceptable law enforcement tool in the eyes of individuals concerned with their privacy, would be to address the legitimacy of the system. As it stands Carnivore disregards privacy rights. Furthermore, since current wiretapping laws do not specifically address surveillance of Internet communications, nor are they applicable by analogy to the telephone system, legislation specifically addressing the interception of Internet transmissions must be written in order to legitimize Carnivore.

Moreover, Carnivore's technical limitations must be rectified. The Carnivore program, in its current states, seems like nothing more than a benchmark project since it is plagued by technical shortcomings. The Carnivore system must be made resilient and reliant in order for it to remain an asset as a law enforcement tool in an era where technology is quickly evolving and criminals are becoming increasingly clever. The FBI must therefore invest personnel and other resources to make Carnivore bug-free, and must refrain from deploying the system until it achieves such robustness.

In addition, Carnivore is currently a burden to the technology industry, since its source code remains secret and its effects to networks undocumented. In order to appease the technology industry's concerns in regards to Carnivore, the FBI should allow and encourage ISPs to handle data interceptions themselves, using their IP sniffer program of choice, as they allow telephone utility companies to wiretap telephone calls. Furthermore, the FBI should release data regarding Carnivore to the public, instead of waiting to divulge such information only after it is leaked to media outlets.

However, even if the FBI makes compromises in regards to Carnivore's deployment and Congress creates legislation specifically addressing the wiretapping of Internet transmissions, appeasing ISPs and individuals concerned with illegitimate governmental surveillance, it would be naïve to believe that the battle to secure individual privacy in the electronic realm had been won. Although Carnivore scandalized the FBI because of its apparent disregard for the constitutional rights of freedom and privacy of Americans, the most invasive breaches of privacy are being conducted by secret organizations and these invasions of privacy remain unknown and cannot be ended by judicial appeals. Thus, no matter what domestic policies regarding Carnivore are put in place, the existence of private communications will continue to be nothing more than an illusion, since ECHELON and other similar systems will continue to monitor them.

No matter what is done to make Carnivore lawful, it can be argued that the right to electronic privacy, a battered cornerstone of modern democracy, has already been lost forever thanks to systems like ECHELON. However, this does not mean that we should sit back, be docile, and allow democratic governments to act without restraint 'in the interests of security'. Although Carnivore is primarily a US system, undoubtedly similar software is in use or, at least, under development, in Canada. We should be ever more vigilant in the face of programs such as Carnivore and ECHELON, policies that lead to legislation such as RIPA, systems like SORM, and a growing acceptance in the face of terror in US for acceptance of a Total [Terrorism] Information Awareness program. As citizens who cherish freedom, we should unite and remind our governments that concerns for public security can rob us of our fundamental right to be free from unfettered governmental surveillance. At the very minimum we should be kept informed of the actions that the state is taking to monitor our communications or systems it is considering to implement. If we see security as part of the struggle to preserve our way of life, the security itself should not repudiate that way of life.

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] J. Goodman, et al, "Carnivore: Will it Devour your Privacy?"(2001) Duke L. & Tech. Rev. 0028.

[4] However, this may change in the US if the Total Information Awareness proposals discussed above are taken forward.

[5] USA., Department of Justice, Carnivore and the Fourth Amendment, (Statement of Kevin V. DiGregory, Deputy Assistant Attorney General, United States Department of Justice, Before the Subcommittee on the Constitution of the House Committee on the Judiciary)(24 July 2000), online: US Department of Justice

http://www.usdoj.gov/criminal/cybercrime/carnivore.htm (date accessed: 24 September 2001) [hereinafter "Carnivore and the Fourth Amendment"].

[6] 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).

[7] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 18 USC. §§ 2510-22

[8] Carnivore and the Fourth Amendment, supra note 5.

[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] Smith, supra note 6.

[11] Ibid.

[12] Goodman, supra note 3.

[13] Ibid.

[14] U.S.A., 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).

[15] M.M. Grier Jr., "The Software Formerly Known as 'Carnivore': When Does E-mail Surveillance Encroach Upon a Reasonable Expectation of Privacy?" (2001) 52 S.C. L. Rev. 875.

[16] Smith v. Maryland 442 US 735, 739 (1979).

[17] See discussion in Goodman, supra note 3.

[18] 47 USC. § 1001

[19] D. Gessel, "CALEA, Carnivore, and Counter-measures"(IS2K Conference, Seoul, Korea, 2000), online: http://www.dis.org/gessel/IS2K/CALEA_Carnivore.pdf (date accessed: 8 February 2002).

[20] United States Telecom Ass'n v. FCC 227 F.3d 450, 453 (D.C. Cir. 2000).

[21] Ibid at 455 (references omitted). See discussion in Grier, supra note 15.

[22] 21st Century Department of Justice Appropriations Authorization Act (H.R. 2215).

[23] R. Longley, "Congress Clamps Down On Carnivore"About.com (6 August 2001), online:About.com http://usgovinfo.about.com/library/weekly/aa080601a.htm (date accessed: 27 December 2001).

[24] Stacy Blasberg "Legal Update: Law and Technology of Security Measures in the Wake of Terrorism" 8 B.U. J. SCI. & TECH. L. 72

[25] D. McCullagh, "Senate OKs FBI Net Spying" Wired News (14 September 2001), online: Wired News http://www.wired.com/news/politics/0,1283,46852,00.html (date accessed: 29 December 2001).

[26] B. Sullivan, "FBI Software Cracks Encryption Wall", MSNBC(20 November 2001), online: MSNBC http://www.msnbc.com/news/660096.asp (date accessed: 27 December 2001).

[27] McCullagh, supra note 25.

[28] Ibid.

[29] Regulation of Investigative Powers Act (U.K.), 2000, c. 23.

[30] Gessel, supra note 19.

[31] K. Lillington, "Irish, UK Crypto Regs Far Apart" Wired News (16 February 2000), online: Wired News http://www.wired.com/news/print/0,1294,34350,00.html (date accessed: 24 May 2002).

[32] Regulation of Investigatory Powers Act 2000, Ch. 23, s. 2 (Eng.). See also discussion in Gessel, supra note 19.

[33] Ibid.

[34] The Economic Impact of the Regulation of Investigatory Powers Bill (The British Chambers of Commerce, 2000) (Editors: I. Brown, S. Davies, G. Hosein), online: The British Chambers of Commerce

http://www.britishchambers.org.uk/newsandpolicy/ict/ripbillsummary.htm (date accessed: 3 July 2002 – no longer online at this site, but held on file) [hereinafter "Economic Impact"].

[35] Ibid.

[36] Regulation of Investigatory Powers Act 2000, Ch. 23, s. 5(3) (Eng.)

[37] Regulation of Investigatory Powers Act 2000, Ch. 23, s. 18(2) (Eng.)

[38] R. Maddocks, "RIP No Longer Means Requiescat In Pace" Le Québécois Libre (1 April 12000), online: Le Québécois Librehttp://www.quebecoislibre.org/000401-6.htm (date accessed: 9 February 2002). For discussion of the Act, see "STAND's Guide to the RIP v1.0"(2 March 2002), online: http://www.stand.org.uk/ripnotes (date accessed: 24 December 2002).

[39] Economic Impact, supra note 34.

[40] Regulation of Investigatory Powers Act 2000, Ch. 23, s. 49 (Eng.).

[41] I. Brown & B. Gladman, "The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses", online: http://www.fipr.org/rip/RIPcountermeasures.htm (date accessed: 24 May 2002).

[42] Lillington, supra note 31.

[43] Economic Impact, supra note 34.

[44] Ibid.

[45] Ibid.

[46] A. Docherty, "U.K. Crypto Law a Key Issue" Wired News (7 March 2000), online: Wired News http://www.wired.com/news/print/0,1294,34776,00.html (date accessed: 24 May 2002).

47 J. Naughton, “Three Minute Guide to RIP” Stand (12 March 2000), online: Stand http://www.stand.org.uk/commentary.php3 (date accessed: 24 May 2002).

48 Economic Impact, supra note 34.

49 Ibid.

50 Ibid.

51 Ibid.

52Docherty, supra note 46.

53 Information Society Commission, “Key Issues : Electronic Commerce”, online: http://www.isc.ie/cgi-local/publications.cgi?f=ecomm (date accessed: 26 May 2002).

54 D. Kelleher, “Legislation Strong on Privacy for Internet” Irish Times 11 July 2000 p 16

55 Ibid.

56 Ibid.

57 Economic Impact, supra note 34.

58 Ibid.

59 Graham, supra note 9.

60 Economic Impact, supra note 34.

61 Ibid.

62 Ibid.

63 See “‘SORM’ to Shutdown?” Cryptome.org Moscow, Russia (25 September 2000), online: Cryptome.org http://cryptome.org/ru-sormshut.htm (date accessed: 13 June 2002).

64 A. Ivanov, “Sorm Problem: Latest News” St. Petersburg Civil Law Center, online: Balfort.com http://www.balfort.com/sorm.html (date accessed: 13 June 2002).

65 Ibid.

66 Larisa Naumenko “Bugging Key in Hostage Battle” The Moscow Times, October 29, 2002

67 Graham, supra note 6.

68 Privacy and Human Rights 2000 : Country Reports : Japan, online: Privacy International, 2000 http://www.privacyinternational.org/survey/phr2000/countrieshp.html (date accessed: 24 June 2002) [hereinafter “Privacy and Human Rights 2000”].

69 Ibid.

70“Wiretap, but Carefully”The Japan Times Online(28 August 2000), online: http://www.snapshield.com/www_problems/Japan/Wiretap_but_carefully.htm (date accessed: 24 June 2002) [hereinafter “Wiretap”].

71 Graham, supra note 9.

72 Wiretap, supra note 70.

73 Ibid.

74 D.A. Laverty, “JAPAN: Internet Privacy and Related Developments” International Counsel (March 2000), online: International Counsel http://www.internationalcounsel.com/pubs/updates/update008.htm (date accessed: 24 June 2002).

75 Privacy and Human Rights 2000, supra note 68.

76 Graham, supra note 9.

77 T. Hamilton, “FBI Software Can Take Bite Out of Canadians’ Privacy” Toronto Star (25 March 2001), online: http://www.efc.ca/pages/media/2001/2001-03-25-a-torontostar.html (date accessed: 13 June 2002).

78 Ibid.

79 Ibid.

80 Ibid.

81 Gessel, supra note 19.

82 Smith, supra note 6.

83 Goodman, supra note 3.

84 Ibid.

85 Smith, supra note 6.

86 Ibid.

87 Ibid.

88 Goodman, supra note 3.

89 Ibid.

90 Ibid.

91 Grier, supra note 15.

92 Ibid.

93 Ibid.

94 Goodman, supra note 3.

95 Grier, supra note 15.

96 U.S.A., 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”].

97 Ibid.

98 United States Telecom Ass'n v. FCC 227 F.3d 450, 453 (D.C. Cir. 2000).

99 Susannah Fox and Oliver Lewis “Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects’ Email and New Laws to Protect Online Privacy” Pew Internet & American Life Project, (2 April 2001)online: http://www.pewinternet.org/reports/pdfs/PIP_Fear_of_crime.pdf (date accessed: 27 December 2002).

100 Lee Rainie, Susannah Fox, & Mary Madden, “One Year Later: September 11 and the internet” http://www.pewinternet.org/reports/toc.asp?Report=69

101 Longley, supra note 23.

102 M. Rothenberg, “FBI’s Carnivore Gnawing at liberty?” ZDNN (11 July 11 2000), online: ZD Net http://www.zdnet.com/filters/printerfriendly/0,6061,2601960-2,00.html (date accessed: 19 September 2001).

103 Stop Carnivore Now, supra note 96.

104 Grier, supra note 15.

105 Smith, supra note 6.

106 Grier, supra note 15.

107 US Senate, The Fourth Amendment and the FBI’s Carnivore Program, (Testimony before the United States Senate – Senate Judiciary Committee by Jeffrey Rosen) (6 September 2000), online: US Senate: http://judiciary.senate.gov/oldsite/962000_jr.htm (date accessed: 26 December 2002) [hereinafter “Fourth Amendment and FBI”].

108 Grier, supra note 15.

109 Fourth Amendment and FBI, supra note 107.

110 Carnivore and the Fourth Amendment, supra note 5.

111 Carnivore Controversy, supra note 96.

112 Fourth Amendment and FBI, supra note 107.

113 Smith, supra note 6.

114 C. Chiu, & B. Steinhardt, “ACL Comments regarding Carnivore review team draft report” American Civil Liberties Union (12 January 2000) online: American Civil Liberties Union http://www.aclu.org/ (date accessed: 25 December 2002).

115 Ibid.

116 Ibid.

117 S.M. Bellovin et al., “Comments on the Carnivore System Technical Review”, (3 December 2000), online: http://www.crypto.com/papers/carnivore_report_comments.html (date accessed: 27 December 2002).

118 R. Stenger, “Universities Unwilling to Review FBI’s ‘Carnivore’ system – Agency’s Restrictions Seen as Overbearing” CNN (6 September 2000), online: CNN.com http://europe.cnn.com/2000/TECH/computing/09/06/carnivore/ (date accessed: 25 December, 2001).

119 Ibid.

120 European Parliament,Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), (A5-0264/2001), online: http://www.fas.org/irp/program/process/rapport_Echelon_en.pdf (date accessed: 20 December 2002) [hereinafter “European Parliament”].

121For reports on Echelon from Zdnet UK, see http://www.zdnet.co.uk/news/specials/2000/06/Echelon/ (date accessed: 20 March 2003).

122 Ibid. See also, “Echelonwatch – Frequently Asked Questions about Echelon” American Civil Liberties Union (7 February 2002), online: American Civil Liberties Union http://www.aclu.org/Echelonwatch/faq.html (date accessed: 26 December 2002) [hereinafter “Echelonwatch”]. It is also clear that nations outside this group run their own systems, such as Frenchelon, see http://www.zdnet.co.uk/news/specials/2000/06/Echelon/ (date accessed: 20 March 2003).

123 N. Hagar, “Exposing the Global Surveillance System” Covert Action Quarterly, online: Mirio’s Cyberspace Station http://public.srce.hr/~mprofaca/Echelon01.html (date accessed: 16 May 2002).

124 J. Bronskill, “Canada a Key Snooper in Huge Spy Network” The Ottawa Citizen (24 May 1999), online: http://insight.mcmaster.ca/org/efc/pages/media/ottawa.citizen.24may99.html (date accessed: 29 May 2002).

125 Echelonwatch, supra note 122.

126 Ibid.

127 Hagar, supra note 123.

128 Ibid.

129 European Parliament, supra note 120.

130 Bronskill, supra note 124.

131 European Parliament, supra note 120.

132 Hagar, supra note 123.

133 Echelonwatch, supra note 122.

134 Hagar, supra note 123.

135 D. Campbell, “Inside Echelon”Telepolis das Magazin der Netzkultur (25 July 2000), online: http://www.telepolis.de/english/inhalt/te/6929/1.html (date accessed: 29 May 2002).

136 European Parliament, supra note 120.

137 Hagar, supra note 123.

138 Ibid.

139 Ibid.

140 Echelonwatch, supra note 122.

141 Ibid.

142 Ibid.

143 Ibid.

144 New Zealand describes the facility, with pictures, on the government website: see Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet Securing? our? Nation's? Safety? http://www.dpmc.govt.nz/dess/securingoursafety/index.html (date accessed: 27 December 2002).

145 Echelonwatch, supra note 122.

146 Ibid.

147 Ibid.

148 European Parliament, supra note 120.

149 Ibid.

150 As related by Mike Frost in CBS's 60 Minutes programme in 2000: "[Thatcher] had two ministers that she said, quote, 'they weren't onside,' unquote ... so my boss went to London and did intercept traffic from those two ministers." See http://news.bbc.co.uk/1/hi/uk_politics/655996.stm (date accessed: 27 March 2003).

151 J. Ashcroft, “Keep Big Brother’s Hands off the Internet”(1997) 2(4) USIA Electronic Journal, online: http://usinfo.state.gov/journals/itgic/1097/ijge/gj-7.htm (date accessed: 27 December 2002).