

16

Privacy and Security: Internet Hacking and Surveillance

Mike Shieh and Krissa Tanthuwani

Internet Hacking and Surveillance Overview

As technology continues to advance, social and ethical issues arise in regards to privacy and security of personal information. Many people are aware of widespread issues in computer technology, such as surveillances and attacks. One major form of infringement on privacy and security is hacking, an unauthorized access into a system in order to gain information. Hacking includes a wide range of activities such as monitoring, thievery, exploitation, altering, vandalism, and destruction of computer systems, all of which endanger individuals' rights to privacy and security. Although this intrusion is frequently associated with negativity, some aspects of hacking can be useful and beneficial towards society. As described later in the chapter, businesses can benefit from ethical hacking, and law enforcement officials can benefit from the skills and knowledge of convicted hackers. The subtopic of this paper describes how the U.S. government can benefit from a form of passive hacking called "Carnivore" or "DCS 1000", an Internet surveillance system that eavesdrops on the public's electronic transmissions. Finally, the rest of the paper discusses how this dynamic nature of technology challenges individuals, businesses, and the government to consider new social and ethical standards regarding personal privacy and security.

Practical Uses and Considerations

Computer hacking is performed to monitor, modify, and/or use the informational content for one's own gain, whether for fun or fraudulent

purposes. A hacker can gain access to a wide range of personally identifiable information that endanger and damage the privacy of individuals, businesses, and government. Information that can be hacked into includes: personal health, financial, and inter-banking information; social security numbers; driver's license data; utility grids; emergency information systems; controls for dams and locks; military communications; and other sensitive information that travels on communication networks such as the Internet (Washington Internet Daily 2003). Although not every attack results in theft or security loss, hackers often cost companies a great deal of time and money (Carnegie Mellon University 1999).

The hacking process is performed by a hacker, a person that uses programming skills to gain illegal access to a computer, a network or a file. This hacker is classified according to his/her primary intentions and level of damage done to individuals and/or businesses. He or she may be benign and has the intention to simply monitor or learn more about the system, without planning to destroy, change, or leave anything behind. Another type of hacker, the information thief, causes more damage because he/she gains access to company or customer information systems, retrieves individuals' personal information, and puts them to his/her own use. This type of hacker provides or sells the stolen information to others for many purposes, including credit card and financial theft, corporate blackmail, or espionage. Lastly, the intention of the functionality thief is to gain knowledge from the interception of web services, then to proceed to alter, wreck, or crash the systems' operation. This type of hacking ranges from basic fun pranks to more serious crimes with the intent of revenge, damage, or the achievement of political and defense corruption (Burgett 2002).

A hacker uses various methods of penetrating through systems to monitor and retrieve personal information, or to crash a system itself. Five different methods are briefly discussed below. First, a denial of service attack (DOS) overloads a network with such a great amount of traffic that it crashes, denying users access to the service. An example of a DOS attack would be the loss of service to a web mail service provider. Second, a hacker may also use Internet Protocol (IP) spoofing as a way of disguising his/her real identity. This method allows a hacker to gain unauthorized access to computers by sending a message to a computer with an IP address showing that the message is from a trusted host. To accomplish this, a hacker must use different tools to find an IP address of a trusted host, and then alter the packet headers so it appears that the packets are coming from the host (Tanase 2003). Third, another technique called Google hacking finds easily exploitable targets and sensitive data on the web by using Google, a powerful search engine used by many people. Google has gained popularity and offers many features, including "language and document translation; web, image, newsgroups, catalog, and news searches" (Long 2004). These features also come with a price, as many hackers use the value of this search engine for bad intentions. Fourth, one of the more common methods of hacking, phishing, imitates the e-mails of legitimate companies. It links recipients to fraudulent websites that were designed to trick people into sharing their personal information. This may include "personal financial data such as credit cards numbers, account

usernames and passwords, and social security numbers.” (Reynolds 2003, p.1). Phishers are usually able to convince up to 5% of targets. Some big name companies that a hacker may imitate are Citibank, eBay, Visa, Washington Mutual, Wells Fargo, AOL, and Yahoo (Anti-Phishing Working Group 2004). Both Google hacking and phishing can often be used simultaneously. Lastly, the phishing method described above is a form of social engineering. With social engineering, a hacker can gain unauthorized access to a computer by deception, tricking the user into providing passwords and other needed information. One popular form of this is the use of deceptive mass e-mails, such as pretending to be a system administrator who needs people’s passwords for important network access.

The widespread fraud and privacy abuses trigger people’s concerns about their own security and the use and control of their personal information. If an identify theft impersonates an authorized user, he or she can inflict damage to the real user’s personal records, credit history, and reputation. Moreover, there exists the fear of political or national threat in which an intruder can break into, damage, steal, and/or act on private information from computer systems worldwide. From a business perspective, hacking causes financial loss when an intruder accesses a company’s web site and web service, linking to sensitive records containing customers’ credit card information, address, and phone numbers. A hacker may be able to alter or damage the data, or use the information to sell to other people or companies. Competitors may also hack a company’s web service to gain reports about potential clients, further using the list of leads for their own business benefit. Hacking also negatively impacts E-commerce, as consumers lose their trust in the Internet as a reliable and secure commerce medium. The result is a loss of sales opportunities for businesses due to the reduction of online transactions.

Additional consequences of hacking include time, money, and human miscommunication costs. A loss of time and money occurs in order to discover, test, apply, and train employees with technology needed to keep computer and network systems secured. The security processes used to ensure privacy include the continuous assessment of systems’ security to identify risks, the evaluation of policies and protection, and the implementation of detection systems such as technology encryptions and firewalls. These processes not only contribute to money costs, but also take away valuable time and may slow down regular businesses. A human miscommunication crisis can also occur and lead to erroneous proceedings. When the victim does not acknowledge that the wrongful incident is a result of hacking, he or she may blame the incorrect person or company that did not actually commit the crime.

From another perspective, hacking may be considered ethical and beneficial to society if it is proven legitimate. Increasingly, businesses and authorities are willing to work with hackers to prevent online attacks and make improvements in computer securities. This type of hacking can be justifiable as long as the hacker has good intentions and commits no theft, vandalism, or breach of confidentiality. The exploration of systems by the benign hacker can be useful because it allows new findings and learning of others’ capabilities. Some hackers

can avoid prosecution and criminal charges by trading in their abilities to help the government protect sensitive computer systems against other hackers, thieves and terrorists. Furthermore, in some cases the government may be willing to pay hackers to search the Internet for vulnerable computer systems, track criminals' online activities, and help make sensitive government networks more secure (Lee 1996).

Another positive aspect of hacking is called ethical hacking, a method used to determine the strength, reliability, and vulnerability of Internet security measures. Ethical hackers use simulations to purposely attack, exploit, or expose the systems to hackers in order to test the security of networks, servers, and applications. This type of hacking is useful in finding and fixing unknown security leaks. Ethical hacking makes it possible for businesses to be better prepared in the case that a real hacking incident occurs. It allows businesses to reduce or prevent the time and costs used to fix damages. It also puts pressure on companies to frequently update their computer systems in order to create and revise more secured networks (Zorz 2003). For example, vendors like Microsoft have a separate department that works solely to prevent people from hacking into their programs. By detecting the methods hackers use, Microsoft has been able to evolve programs to stop this dilemma (DiDio 1998).

Analysis of Internet Surveillance Via "Carnivore" or DCS 1000"

On July 11, 2000, the U.S. Federal Bureau of Investigation (FBI) announced its use of an Internet surveillance system called "Carnivore", or "DCS (Digital Collection System) 1000." The system is a computer-based application installed with an Internet Service Provider (ISP) to intercept and collect the electronic transmissions of criminal suspects. The FBI uses Carnivore as a form of passive hacking tool to keep track of individuals that execute their criminal plans through cyberspace. By installing these "black boxes" on the main network, the government can increase law enforcement by connecting directly to the public's Internet traffic. This surveillance has been beneficial since it has helped secure the convictions of thousands of felons. However, opposing viewpoints exist within the society since the usage of such a system generates ethical and privacy concerns.

From the beginning of Carnivore's invention, the main mechanics have been kept a closely guarded secret. No information about the first version was made to the public, but there were speculations that this first version was in fact a readily available commercial program called Etherpeek. In 1997, the second version was created with the name of Omnivore. According to the very little reports given by the FBI, Omnivore's purpose was to "look through e-mail traffic traveling over a specific ISP and capture e-mail from a targeted source, saving it to a tape-backup drive or printing it in real-time" (Mycrypto 2004, p.2). This system was used until 1999, when it was replaced by a more advanced structure called the Dragonware Suite. This structure contained added features, such as the capability to download files and web pages from suspected criminals, and better developed software to search e-mail messages. Dragonware encompasses three parts: Packeteer, Coolminer, and Carnivore. Packeteer, on which there has been no official information released, appears to be an application for reassembling

packets into cohesive messages or web pages. Coolminer, on which there has also been no official information released, is most likely an application for extrapolating and analyzing data found in the messages. Although there has been no official information on Paketeer or Coolminer, the Carnivore feature has been used since the Cold War, where the U.S. Navy was able to “tap into Soviet undersea fiber optic lines by using special submarines, and gain complete knowledge of that set of communication” (Mycrypto 2004, p.2). Since then, Carnivore has thrived to become a main form of government Internet surveillance today (Tyson 2002).

Implementation and Usage

Carnivore uses a Windows NT/2000-based system that captures information through a form of packet sniffing. A packet sniffer is a form of technology used by computer administrators to monitor networks, perform diagnostic tests, and troubleshoot problems. Sniffing programs exist in two forms, either as commercial packet sniffers used to help maintain networks, or as underground packet sniffers used to break into computers. In the case of Carnivore, a packet sniffer is a program that plugs into computer networks and enables a person to view all traffic information passing through. Each packet is “sniffed” as the program carries information to the viewer, without interfering with any of the information. A packet sniffer can be set up in two ways: unfiltered, which captures all the packets, or filtered, which captures only the packets that comprise of specific data. In the case of Carnivore, a filtered system is used to capture only the targeted individuals’ transmission. After the intended packet is found, the data is copied and then stored in memory or on a hard drive (Tyson 2002).

The process of setting up the Carnivore system involves four stages: installation, filtration, segregation, and collection. Before any of the stages, the FBI needs to receive judicial approval. Once approved, they check to see if the suspect’s Internet Service Provider has the technology to comply with the court order. If not, the FBI cooperates with the ISP technicians to place Carnivore in the network where the suspect’s communication packets can be isolated. Once cooperation with the ISP is achieved, the initial filtering is set up. During this process, Carnivore monitors all the ISP traffic from both targeted and non-targeted individuals, then proceeds to filter the packets at the ISP’s designated speed. Carnivore takes a picture each second, searching for the suspect’s information. If the suspect’s information does not exist, the packet automatically disappears and is not collected, stored, or saved. If there are traces of information, Carnivore proceeds to the third stage (Dunham 10). The third stage consists of segregating the suspect’s information. Once detection has been made, the packets containing some traces of the suspect’s information are then segregated for additional filtration and storage. This leads ultimately to the last stage of collection, which involves more filtering of the suspect’s information. Carnivore then collects and processes the final information that can be used according to the court order, discarding any non-retrievable information (Dunham 11).

A defense method that individuals can use to protect their privacy is through encryption technology. A personal computer (PC) can

encrypt messages with codes that are difficult to break. Officials may monitor a suspect's online communications and sniff up the data, but they are not able to understand this encrypted information. The most popular encryption uses online key systems, known as the public-key encryption. A user issues a public key that others can use to send the user a message, which can be decoded only with the user's private key. To overcome this, law-enforcement officials have advocated the use of different software that use a "back door" feature to read the encrypted e-mail or files of criminals. However, it can be argued that allowing back door software would actually weaken codes used for Internet security, which hackers and criminals could exploit (Weber 2001). Nonetheless, the point still stands that if material is encrypted, the individual is protected from the government's intrusion to some extent because it is generally difficult to break the encryption.

The Positive Aspects of Internet Surveillance

Millions of people around the world use the Internet. With the infinite knowledge and possibilities it provides, the Internet can definitely be utilized to connect people to one another and/or make everyday tasks easier. However, many people are unaware of the prospective perils the Internet has. "The rise of the Internet, with e-mail, instant messages, and more, has opened gigantic pipelines for all to use, including criminals" (Weber 2001). These criminals view the internet as the perfect way to commit crimes, to con individuals, or to affect millions of people through cyber-terrorism. Criminals also use e-mail to spread information to other criminals since the process is convenient and fast. This is where the Carnivore system comes in: it keeps an eye on these hazardous people to put a stop to their evil intentions. That in itself, Carnivore is a form of passive hacking used to detect the "real" illegal hackings and other wrongdoings. Carnivore is used by the FBI in five areas: cyber-terrorism, information warfare, child pornography, fraud, and virus writing.

Terrorism is a great threat throughout the world. Particularly in the United States, cyber-terrorism can be devastating because of the society's reliance on computers. Cyber-terrorists have the capability to shut down national infrastructures like energy usage, transportation, water, and telecommunications as a means to intimidate and harm the society. Carnivore attempts to stop or hinder terrorism by monitoring and supervising the internet activities of known terrorist groups, with procedures equivalent to tapping phones lines (Dunham 2004). While testifying on the worldwide threat of terrorism, George Tenet, the Director of Central Intelligence, states that "terrorist groups, including Hizbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qu'ida organization, are using computerized files, e-mail, and encryption to support their operations" (Dunham 2002, p.4). These organizations have yet to succeed terrorizing America through cyber terrorism; however, the potential threat is still greatly present. This is the very reason the FBI sees Carnivore as a necessity, because the system makes it possible for officials to monitor activity and prevent any catastrophic tragedies from occurring. There have already been early signs of promise, such as when the FBI discovered that e-mail was a major method used for communication for a terrorist group. Thus, the

FBI was able to stop this group from stealing explosives from National Guard Armories in several southern states. It was also discovered that this same terrorist group used the Internet to download information on Ricin, the 3rd deadliest toxin in the world. In instances like this, Carnivore can follow the steps of terrorists and stop them before they strike (Dunham 2002).

Next, Carnivore is helpful when tracking down those individuals that intend to use information warfare against the United States. Information warfare is a subcategory of cyber-terrorism. Since many nations cannot measure up to America's power in terms of military strength, they seek information warfare as retaliation. "This type of war attempts to exploit our 'Achilles heel,' a national dependence on information technology in government, commercial, and private operations." (Dunham 2002, p.4). A book published by two Chinese military officials explains that the use of unconventional techniques, such as spreading computer viruses, is the only way to neutralize the United States. Moreover, the Russian government has been known to think along the same lines. Russian government officials acknowledge that attacking America's computer infrastructure could lead to the same result as using weapons of mass destruction; either way hurts the United States immensely (Dunham 2002).

Another crime that Carnivore prevents is child pornography. Even though this is not a national security threat, it is destructive to communities and society. The offenders may download graphics from child pornography websites and/or use the Internet as a device to arrange meetings between themselves and young children. This can lead to violent and sometimes deadly consequences. "Between 1995 and 2001, the FBI investigated over 800 cases involving offenders crossing state lines to carry out an illegal sexual relationship and more than 1,800 cases involving the exchange of child pornography over the Internet" (Dunham 2002, p.5). It is vital to track these people because they have the tendency to victimize repeatedly. Studies have shown that a child molester typically abuses approximately 70 children in his or her lifetime (Dunham 2002). With the help of Carnivore, the FBI devised a plan to capture these sexual predators through processes such as "Innocent Images." This site is intended to capture those who distribute child pornography with the Internet. A FBI agent will go undercover as a child over the internet and lure sex offenders to meet with them, allowing the agent to arrest and prosecute the criminal (Dunham 2002).

Fraud is an issue that countless Americans have encountered. The Internet is ideal for fraud for three reasons. First, people can be easily targeted with the amount of features that it offers, such as chat rooms, instant messages, e-mails, and forums. A person can look up names, addresses, and e-mail addresses through a directory and start sending out spam e-mails. Secondly, individuals can remain anonymous. When a person creates a website selling defective materials that do not actually work, he or she may experience fewer, if any, consequences because his or her real identity is kept secret. It is difficult to trace the real identity of the creators of millions upon millions of web sites that can be found. "The critical difference in fraud committed over the Internet is that the perpetrator can 'virtually' vanish, leaving consumers wondering to whom or where to turn to for help" (Dunham 2002, p.6).

Thirdly, those that commit fraud do not face expenses with obtaining a toll-free number, mail, and/or hiring people to maintain the mail. Since they can sign up for free email with companies like Yahoo and Hotmail and obtain a screen name for instant messages with AIM, these previous expenses are no longer necessary. According to the North American Association, Internet related fraud estimates to be about \$10 billion per year. In one meticulous case in 2000, 19 individuals implemented an insider trading scheme, where a person with stock information passed along tips to firms through chat rooms. These 19 people were accused of fraud and discovered to have pocketed several million dollars worth of illegal money. Had Carnivore been in place at the time of this occurrence, they may have been caught sooner than through traditional methods (Dunham 6).

Finally, the spreading of computer viruses is becoming increasingly perilous. Viruses can be detrimental to company and government computer systems, hurting individuals who simply open an e-mail. Viruses such as the Melissa Macro Virus and the Explore.Zip worm have destroyed individuals' computer files and programs around the world. They can entirely shut down email systems and delay communications. For example, in some incidents, Microsoft had to put a halt to all outgoing e-mails throughout the company (Briody 1999). A hacker can also spread a virus to a company to destroy its database, which often holds immeasurable valuable information. This can be costly and some of the data lost may never be recovered.

All things considered, this new program will eventually be able to do exactly what it was invented to do: monitor, track, and prevent criminals from breaking the law; protect potential victims from facing harmful consequences, and give society assurance that the world is safer place. Even with the loopholes found in Carnivore currently, the overall benefits this plan offers can outweigh its negative aspects. Since this program has recently been revealed and is relatively new, the public will have to wait and see if the FBI and government officials can keep their word on its potentials.

The Negative Aspects of Internet Surveillance

Evidence suggests that Carnivore may be powerful, but it still has several shortcomings. At the first glance, the name "Carnivore" alone suggests a negative connotation. The fact that Carnivore is for wiretapping and spying on citizens raises the public's concern. It has drawn significant criticism from civil rights groups. The main critics of Carnivore are the Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU), two public interest groups devoted to civil liberties issues. On July 11, 2000, EPIC sued the FBI under the Freedom of Information Act (FOIA). It pursued the public release of Carnivore's background information, source code, technical details, and the potential privacy issues of the technology. The group was able to obtain some information and records, although the FBI still refused to turn over Carnivore's source code and some of its inner workings. The secrecy surrounding exactly how Carnivore operates causes the public, IT managers, and ISPs to feel ambiguous about its implementation. The public is also generally unclear the activities between the intelligence agencies and law enforcement. Many people

have confused the Carnivore system with the "Echelon" system, a global mass surveillance system used by intelligence agencies. Hence, EPIC's general counsel David Sobel argues that "Carnivore's use should be suspended until the questions surrounding it finally can be resolved. There's a great deal about Carnivore that we still don't know" (Dunham 2002).

The main privacy concern is that the government and the FBI can misuse Carnivore by examining more data than their court orders permit. In other words, it can do a broad sweep and spy on all individuals' Internet traffic and emails. Carnivore's intended function is to track and record E-mail subject headers, URLs, and IP addresses, but not the actual contents of an E-mail. Donald Kerr's statement to the U.S. House of Representatives is that Carnivore "does not search through the contents of every message and collect those that contain certain key words like 'bomb' or 'drugs'" (Accelerated Promotions 2004, p. 2). EPIC's legislative counsel Chris Hoofnagle says that although the government claims to only monitor data traffic's subject headers, the real interceptions often include more substance. The FBI moves beyond the scope of a search warrant because it also has access to other information such as message size, time of transmission, the number of jumps that a message takes to reach its destination, and other valuable data that can be extracted (Armstrong 1996).

Although the FBI states that Carnivore does not have the capacity to monitor every single individual's emails and that the monitoring is only restricted within the court's terms, the public has no actual way of knowing whether the FBI will misuse their power or exactly what Carnivore is capable of. Carnivore's intended function is to filter the data traffic and only retains the relevant data. The system should have the ability to distinguish between communications that have or have not been authorized for interception. For instance, Carnivore can be configured to intercept e-mail but not online shopping records. However, the software does not always work correctly. In some circumstances, the system picks up both the authorized and unauthorized interceptions (Olavsrud 2002).

The reason that the system is not as selective with the data captured as the FBI has claimed is due to several imprecise technical functionalities. The controversy over Carnivore comes from the fact that communications through the Internet and the phone are different. In phone communications, a direct connection exists between two parties. However, Internet communication is broken up into tiny packets, which mixes together pieces of many different conversations. Consequently, extracting one person's data often involves inspecting the data of many others as well. Overall, there is not enough confidence to ensure that Carnivore will only pick up the intended traffic (Accelerated Promotions 2004). The intercepted data may be misinterpreted if a single packet is dropped, repeated, or miscategorized. Dynamic IP addresses also make it difficult to identify which computer the data is coming from. Additionally, since ISPs vary in their architecture, the system's components may work in one system's architecture but fail in others. ISPs and IT managers are also concerned that the system may damage the company's technology infrastructure. Lastly, the possibility

of hacking exists since Carnivore is controlled remotely and has open security holes.

Since the Carnivore system also intercepts unnecessary non-targeted content, it may have blocked the actual targeted criminal investigations. The unauthorized interceptions not only violate an individual's privacy, but also disrupt or delay anti-terror investigations. For example, in March 2000 the system was unable to perform effectively under the FBI's International Terrorism Operations Section (ITOS) called "UBL Unit," which refers to the government's official designation of Osama Bin Laden. The Carnivore system was turned on, but it blocked the actual surveillance of the target by also picking up electronic communications of on non-targeted individuals. By this, critics have argued that the FBI is unable to effectively manage foreign intelligence surveillance activities (Electronic Privacy Information Center 2002).

Privacy advocates are also concerned that Carnivore violates the Fourth Amendment of the Constitution. The central purpose of the Fourth Amendment is to protect the public's privacy and security from the government's unreasonable invasion. Law enforcement must obtain warrants of probable cause or suspicion in order to conduct searches and seizures. However, law enforcement is allowed to conduct searches without these warrants under limited circumstances, such as those involving government issues. In other words, the government's interest can outweigh an individual's expectation of privacy. An example is the pen-trap order, in which a probable cause is not needed to obtain a suspect's information. In criminal cases, a court order allows the interception and collection suspects' Internet transmissions without the suspects' knowledge or consent. However, at the same time, the system is given access to the data of those individuals that are not suspects. In the case that the system does capture the data of someone's illegal activity, to a certain extent that information may still be used as evidence in prosecution (Greene 2002).

Furthermore, an issue concerning property arises in regards to who has the ultimate control of the system. Responsibility may be divided between the government that uses the system for surveillance, and the technical agents that install and operate the system. In this case, the technical agents are the ones that must configure the system properly so it does not collect data beyond what is permissible by the laws and court orders. The downside is that Carnivore does not have an auditing function to keep track of individual users' identities. The system logs all users on as 'administrator' and gives everyone full access to all resources. In other words, if an agent changes the settings of Carnivore, it would be difficult to determine the actual person guilty of violating the restrictions. Whether the deed is intentional or due to error, the result is an over-collection of data instead of just the restricted data. The system still needs improvement with stricter controls and independent monitoring, where individual users can be held responsible for their actions within the system.

Ethical Analysis and the Future

Internet technology has grown tremendously over the past decade, and the same growth will continue to persist into the future. Cyberspace

is accessible to a wide range of members in society, including those with criminal intents. With this growth, the United States government has placed more limits on individuals' privacy and promoted the more extensive use of electronic surveillance. Furthermore, the September 11th terrorist attacks have rapidly increased the pace of security measures all around the world. In the United States, law enforcement officials are given even greater power to conduct communications interceptions. The Patriot Act allows the use of Carnivore Internet surveillance technology without a judicial warrant but only a court order. The warrant requirements needed for monitoring have been reduced, allowing government officials easier access to individuals' records. In addition, the government is promoting policies that require developing communication technologies to have built in surveillance capabilities, and is also seeking limits on devices that provide encryption (Electronic Privacy Information Center 2002).

The Carnivore system's primary intention is seemingly a responsible and necessary approach to assist the law enforcement in capturing criminals. However, while it can protect the citizens' security, the government must also consider its ability to invade on the citizens' privacy. Many people believe that electronic surveillance must be limited to only unusual circumstances, since they are a highly intrusive form of monitoring. The controversial aspect of this issue is that governmental actions can never be equally supported by all viewpoints. When an investigative method such as Carnivore is used, privacy advocates criticize the government for invading the public's privacy rights. On the other hand, when there is a failure to eliminate a potential criminal threat, crime control advocates criticize that the government for being negligent in its regulation of social welfare.

As technology advances, the government can no longer use existing standards to manage the surveillance of communications. Due to the changing disposition and sensitivity of personal information, it is important to provide protection for individuals' privacy and human rights. Consequently, the government must be able to effectively apply new laws, policies, and standards to keep up with the changing technologies. The government has to decide the most appropriate method to increase the nation's security while maintaining a level of freedom and privacy for individuals. The Electronic Communications Privacy Act (ECPA) clarifies how existing wiretap laws can be applied to Internet surveillance and sets boundaries on how much the government can invade the citizens' online privacy. As long as the Carnivore system is used within the constraints and guidelines of ECPA, it has the potential to be a useful weapon against criminal and national security threats (Electronic Privacy Information Center 2002).

Due to the new anti-terrorism and security legislations, the level of Internet monitoring by the government will probably not decrease. Several methods can be used to protect the security and privacy concerns of individuals that are monitored by this Carnivore system surveillance. First, technical changes must be considered to address the problem. Improvement of Carnivore's configuration is needed so that it only extracts the intended data traffic. This will reduce the system's possibility of invading into non-targeted individuals' privacy, and not jeopardize other important investigations, such as those involving

terrorism. Second, specific identifications are needed to distinguish FBI agents operating on the system. This way, agents are responsible for any mishaps, such as the change of control settings to collect more data than the system is intended for. Third, many countries now require the public information reporting about the use of surveillances by the government agencies. The FBI should disclose more about the systems' internal workings so there is not such a secrecy surrounding exactly how it operates. This way, the public can alleviate their security and privacy concerns once they become more aware about the functions of the Carnivore system (Electronic Privacy Information Center 2002).

Conclusion

The explosion of the Internet and computer networks allows individuals, businesses, and governments to find and store valuable information, communicate to one another, and enjoy the unique methods of making their lives easier. However, this also makes it possible for anyone to perform illegal actions and misuse the powerful technology through a variety of means. The changing nature of technology and the sensitivity of information raise the standards needed to protect the privacy and security of individuals. These standards include greater security consciousness among all computer system users, as well as tougher security measures and more stringent laws. The outcome of Internet hacking and surveillance may seemingly appear negative, but these methods also consist of positive aspects that are beneficial towards society. As mentioned above, businesses can benefit from ethical hacking, which uses simulations to purposely attack the systems in order to test the security of networks, servers, and applications. This process tests the strength and vulnerability of Internet security measures and prevents the time and monetary costs used to fix the incurred damage. Additionally, law enforcement officials can benefit from the skills and knowledge of convicted hackers. The previous offenders can assist companies and law enforcers in the fight against other dangerous offenders, and may help advance society's knowledge of technology. Finally, the U.S. government can benefit from the Carnivore passive hacking, since it functions to capture criminals that conduct their plans over the Internet.

The reduction of privacy for the sake of greater security remains a controversial topic. The opinion and morality of the subject depends on an individual's personal judgement and stems from his or her own culture. From one perspective, it may be reasonable for the government to restrict society's freedom and privacy in order to protect its citizens. From another perspective, hacking and surveillances remain an intrusion of individuals' privacy. As a result, individuals and businesses lose their sense of confidentiality and feel the need to heighten their sense of protection towards their personal information. If one believes that hacking and surveillances should be allowed, questions arise as to what level it must reach before it is considered unethical. In regards to the principles of decision-making, an ends-based thinking may be applicable if the consequence is the greatest good for the greatest number. The assistance from ethical hacking and Carnivore Internet surveillance may very well outweigh the costs of many crimes. If the benefit is greater than the cost, then the processes

can be successfully utilized in a more productive manner. However, above all else technology should only be applied with strict regards to maintaining the public's privacy and security. In the end, it is up to the society to consider the social and ethical standards to apply to the ever-changing technology, so valuable information does not fall into the wrong hands for the wrong purposes.

Works Cited

- Anonymous. "Is Government Internet Monitoring Out of Control." *The Secured Lender*. Oct 2002: 76.
- "Anti Terrorism Technology: Carnivore -Surveillance System." 2004. 03 *Accelerated Solutions*. Nov 2004 <<http://acceleratedpromotions.com/consumerelectronics/usa-patriot-act-carnivore.htm>>.
- Armstrong, Del. "Social Engineering." 25 Oct 1996. 08. Sept. 2004. <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html>
- Briody, Dan. "Massive e-mail virus outbreak spreads like wildfire." 29 Mar 1999. CNN. 01 11. 2004 <<http://www.cnn.com/TECH/computing/9903/29/melissa.idg/~hsindex.html>>.
- Burgett, David. "Keeping hackers out of your Web services." 14 05.2002.*Builder.com*. 05 May 2004 <<http://insight.zdnet.co.uk/internet/security/0,39020457,2110160,00.htm>>.
- "Computer Hacking and Security." 2004. *MyCrypto.net*. 06 Sept 2004 <<http://www.mycrypto.net/underground/hack.html>>.
- "Computer Hacking and Security." 1999. Carnegie Mellon University. 08 Sept 2004 <http://www.cert.org/tech_tips/denial_of_service.html>.
- Dempsey, James. "Opinion--face-off: Does carnivore go too far?." *Network World Framingham*. 10 Oct 2003: 73.
- DiDio, Laura . "Want to prevent break-ins? Just ask a hacker." 02 03.1998. *Computerworld*. 06 Sept 2004 <<http://www.computerworld.com/news/1998/story/0,11280,29982,00.html>>.
- Dunham, Griffin. "Carnivore, the FBI's e-mail surveillance system: Devouring criminals, not privacy." *Federal Communications Law Journal*. 5.2002: 543-566.
- "FBI's Carnivore System Disrupted Anti-Terror Investigation." 28 May 2002. Electronic Privacy Information Center. 028 10.2004 <http://www.epic.org/privacy/carnivore/5_02_release.html>.
- Greene, Thomas. "How Carnivore Works." 19 Dec 2002. *The Register*. 02 11.2004 <http://www.theregister.co.uk/2000/12/19/how_carnivore_works/>.
- Kahaner, Larry. "Hungry For Your E-mail." *Information Week*. 23 Apr 2001: 64.
- Lee, J.A.N.. "Hacking - Encyclopedia Description." 14 10.1996. 08 Sept 2004 <<http://courses.cs.vt.edu/~cs3604/lib/Hacking/MacMillan.Hacking.html>>.
- Long, Jonny. "Google Hacking Mini Guide." . 07 05.2004. Informat. 07 Sept 2004 <<http://www.informat.com/articles/article.asp?p=170880>>.
- Noguchi, Yuki. "Online Search Engines Help Lift Cover of Privacy." *The Washington Post*. 09 02.2004. A01. 04 Sept 2004 <<http://www.washingtonpost.com/wp-dyn/articles/A24053-2004Feb8.html>>.

Olavsrud, Thor. "Carnivore devours more than it lets on." . 29 May 2002. *Internet News*. 02 11.2004 <<http://www.internetnews.com/busnews/article.php/1146651>>.

Reynolds, Chris. "Bank to use SMS messages to check transactions." 05 Oct 2004. *Computer Weekly*. 07 09.2004. <<http://www.computerweekly.com/Article133-971.htm>>.

Tanase, Matthew. "IP Spoofing: An Introduction." *Security Focus*. 11 Mar 2003. In Focus. 08 09.2004 <<http://www.securityfocus.com/infocus/1674>>.

Tyson, Jeff. "The Process." 2002. *How Stuff Works*. 03 Nov 2004 <<http://computer.howstuffworks.com/carnivore3.htm>>.

Weber, Thomas. "A Primer on Technology That Has the Potential to Help Foil Terrorism." *The Wall Street Journal*. 9 17. 2001: b.1.

"What is Phishing?" 2004. Anti-Phishing Working Group. 06 Sept 2004 <<http://www.antiphishing.org/>>.

Zorz, Mrko. "Using Ethical Hacking to Ensure Security." 09 Jul 2003. HNS. 09 09.2004 <<http://www.net-security.org/news.php?id=3075>>.