Privacy and Surveillance: The Carnivore case

An in-process version for the computingcases.org website

Privacy: Machado and Carnivore

Version 1: Begun 07/25/05 by William J. Frey
Completed: 09/15/05 by José A. Cruz-Cruz

Based on writings in www.computingcases.org prepared by Chuck Huff and Bill Frey and class documents from University of Mayaguez, PR, FILO 3185 prepared by Bill Frey

Abstract

Carnivore, a packet sniffer used by the FBI to eavesdrop on criminal and terrorist online activity, was developed in the late 1990's out of an earlier prototype, Omnivore. Carnivore advances on its predecessor by zeroing in on the cyber activities of its target. Omnivore "ate" everything in its path and collected too much information; Carnivore gets right "to the meat".

Carnivore is used to gather intelligence for domestic security and assemble evidence for criminal prosecution. With an authorizing court order in hand, the FBI installs it on an Internet Service Provider to trace the online communications of suspected individuals. Carnivore offers features that gather material ranging from the headers of email ("to and from" information) to their full content. The extent and range of the surveillance comes from the court order and the purpose of the surveillance. The FBI takes the court specifications and configures Carnivore to carry them out to the letter. In this way, its proponents argue, it can be specifically tailored to balance the surveillance needs of law enforcement officials with citizens' civil rights.

Carnivore's appearance sparked opposition from civil rights groups such as the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC). It even inspired a special website, www.stopcarnivore.org. Criticisms ranged from concerns that Carnivore violates citizens' civil rights (privacy and due process) to claims that it is part of a larger conspiracy to bring the Internet under centralized control.

9-11 has had its impact on Carnivore. To nip terrorism in the bud, Congress passed the Patriot Act which lowered thresholds for surveillance approval and greatly expanded its range. Carnivore, a powerful surveillance tool prior to 9-11, became much more powerful in the new legal context of the Patriot Act.

The narrative below plus supporting documents will provide Carnivore's history, summarize opposition, describe technical components, and set forth the underlying legal context (including the Patriot Act). Ethical reflections include the intermediate moral concepts of security, privacy, and due process.

Historical Narrative

Introduction

9-11 created shock waves that rippled throughout our lives. It dramatized how planning, coordinating, funding, and recruiting for terrorist activities now take place online in computer mediated environments. Defending against terrorism requires developing defensive computing tools that counteract the offensive tools used by terrorists and criminals.

But these defensive weapons have their own impact. Responding to cyber terrorism and cyber crime require rebalancing security with basic civil rights like privacy and due process. Historically these two sets of considerations have been at odds with one another. Enhancing surveillance increases security but undermines privacy and due process; elevating privacy and due process undermines security. Because computing instruments human action (ref), it will come to play a vital role in choosing and designing the post 9-11 world. Computing offers technologies that could instrument radically different designs for this world:

1. Indiscriminate use of computer-enhanced surveillance devices could create a transparent world that resembles Bentham's Panopticon. In this world nothing would be private; everything would be laid bare to centralized observation and control.
2. Widespread use of encryption systems could create impenetrable zones of privacy that will allow criminals and terrorists to wreak havoc anonymously and with impunity.
3. Computing skills working hand in hand with moral virtues could provide innovative designs that would integrate security with civil rights like privacy, and due process.

Exploring these options sets the context for the Carnivore case.

By creating a wall in cyberspace that protects individuals and hides their activities, encryption can enhance privacy. Individuals enter cyberspace anonymously under multiple identities enabling them to act boldly without accountability. Encryption could shield online activities from outside inspection which would provide terrorists, criminals, hackers, spies, and disgruntled employees a protective space in which to carry out their harmful activities. Financial services, businesses, public utilities such as water and power, and essential government services all depend on computing in ways vulnerable to disruption from online criminal and terrorist activities like hacking. Computing, because it instruments human action, magnifies the impact that criminals and terrorists can have. So privacy backed by encryption could produce a dystopia where innocent individuals are rendered vulnerable to the cyber activities of criminals, spies, and terrorists.

But, as the material presented below will show, computing could also empower invasive surveillance of online communication. Computer-enhanced surveillance tools such as Echelon, Biometrics Technology (e.g., Face Recognition Devices), Key-logger systems, Fingerprint Scanning, and Thermal-imagining systems can be used to monitor, incriminate, and control "suspicious individuals". (See the table below for more on these

surveillance technologies.) In the hands of ruthless and overzealous law enforcement officials, computer-aided technology could be used to engage in all kinds of fishing expeditions, all the more invasive because of the way in which computer technology enhances their range and power. So computing technology can empower invasive surveillance, and history shows us that there will always be individuals willing to use these powerful devices for morally and legally questionable ends. Technological checks (encryption) combined organizational checks (supervisory control and judicial oversight) help somewhat but are still fallible. This second dystopia, the opposite of the first, would issue in Bentham's Panopticon where all human action is rendered transparent to impersonal, centralized, controlling authority.

Insert: Computer-Aided Surveillance Technologies

Technology	Description
Echelon	Secrete international surveillance network in place since 1978. British Intelligence and the NSA are major players. Able to scan email and wireless content in foreign countries.
Face Recognition Technology	Biometrics technology that can digitally analyze biological characteristics such as facial structures and iris patterns. Minority Report shows this in a fictionalized setting. (See Boyer at Notre Dame)
Key-logger system	Captures keystrokes on a computer to uncover encrypted passwords
Fingerprint scanning	"Biometrics technology prints and transmits fingerprints electronically to identify people"
Thermal-imagining system	Used in the Kyllo case to discover a marijuana growing facility inside a private individual's house. It can "display pictures of invisible heat waves given off by objects in criminal investigations

Source: Privacy vs. Safety: Terrorist threat shifts priorities in online rights debate By Stefanie Olsen and Evan Hansen at CNET News.com on September 17, 2001

Between security without privacy and privacy without security, the FBI offers what it considers to be a compromise, Carnivore. (Carnivore's critics question this as the material presented below will show.) A packet sniffer programmed to eavesdrop on criminal and terrorist activity, Carnivore was developed in the late 1990's out of another program named Omnivore. Carnivore offers flexible features that can capture as little as the headers of email (the attached "to and from" information) or as much as their full content. The extent and range of the surveillance comes from the court order and the purpose of the surveillance. In short, Carnivore promises to tailor surveillance to achieve security without threatening the privacy of innocent individuals. It promises to avoid both of the above-mentioned dystopias by synthesizing security with basic civil rights like due process and privacy.

Historical Background
In his testimony before the United States Senate, The Committee on the Judiciary (September 6, 2000) FBI official, Donald M. Kerr, described a frightening future for the Internet:

> By now, it has become common knowledge that terrorists, spies, hackers, and dangerous criminals are increasingly using computers and computer networks, including the Internet, to carry out their heinous acts. In response to their serious threats to our Nation, to the safety of the American people, to the security of our communications infrastructure, and to the important commercial and private potentialities of a safe, secure, and vibrant Internet, the FBI has responded by concentrating its efforts, including its technological efforts and resources, to fight a broad array of Cyber-crimes.

Cyber crime, including identity theft and child pornography, is still on the rise. Spies have become adept at hacking into confidential government and industrial information. *Cyber* terrorism has emerged as the new species of an old genus because much of the work of terrorists (recruiting, researching, communicating, coordinating, and fund raising) now takes place online. The vast information available on the Internet that computing technology scoops up combined with the veils of anonymity and encryption it provides, have made terrorists bolder and more effective.

Introducing new technology into a socio-technical system upsets preexisting balances and creates value mismatches that need readjusting. The introduction of the telephone required designing devices for electronic surveillance to control telephone-aided criminals; wiretaps, traps and traces, and pen registers provided law enforcement officials with weapons to fight back against these criminals. Likewise, defending against cyber terrorism and cyber crime require new cyber tools to match those of the criminals.

The FBI claims to offer just such a weapon in Carnivore. At first Carnivore and Omnivore were used secretly. But news leaked out to the press, and the FBI had to deal with a public relations problem brought about, in part, by the name of their new system. Carnivore is a packet filter or "sniffer". Commercial and freeware packet sniffers had been in circulation before Carnivore. Internet Service Providers, for example, use these tools to detect denial of service attacks, as diagnostic software to monitor quality of communication, and to filter out ever unpopular spam. Data mining software, already notorious for its potential to invade privacy, contains filtering techniques that could be used for Carnivore-type purposes. But critics, remembering how the FBI had abused civil rights during the tenure of Hoover, feared more of the same. The veil of secrecy surrounding Carnivore and the name itself created a pervasive environment of distrust that the FBI had to counteract.

How does Carnivore work?
Email and the exchange of information online are based on packet sharing. Information in email is divided into packets before it is sent to its final destination. Each packet

contains destination and reassembly information. Packets, then, are routed to their destination via different paths to avoid Internet traffic jams. At the final destination, programs reassemble the packets into their original form using the embedded information contained in their headers.

Special software, called packet filters or sniffers, identify, select, and capture specified packets for various purposes, one of which is surveillance. Commercial filters such as Net ICE and EtherPeek predate Carnivore and Omnivore. In fact, commercial developers claim their product is superior because it avoids the programming shortcuts that the FBI may have taken to rush its packet sniffer into use (ref). (Whether the FBI took these programming shortcuts is a contentious issue since the FBI has withheld Carnivore's source code.) Freeware versions like TCPDUMP also exist. In all probability, the FBI built Carnivore out of commercial packet filters, adding configuration flexibility to make Carnivore responsive to judicial overview. Carnivore is a part of the DragonWare software package. After it filters packets from the Internet stream, other programs (Packeteer and CoolMiner) create higher level packets and display the data for FBI agents in a Web Browser.

The following summarizes the procedure the FBI uses to put Carnivore into action:

1. *The FBI receives court permission* (in the form of a court order to an Internet Service Provider) *to conduct surveillance on a suspected individual*. To get this order, they must present a justification to the court that meets certain thresholds. The court order issued then specifies the communication that can be captured and the duration of the surveillance.
2. *The strictness of the threshold requirements the FBI must meet depends on the information sought and the purpose of the surveillance*. "Threshold requirements" refers to the standards that must be met before the court will allow surveillance. It specifies the **information** that can be collected (its range and content) and the **purposes** for which it can be used. The more detailed the information, the higher the threshold, i.e., the higher the burden of proof the court places on the investigator to justify the surveillance. Information collected for intelligence purposes has a lower threshold than information that will be used as evidence in a criminal prosecution. These thresholds exist to balance civil rights with security concerns and criminal prosecution interests.
3. *The FBI takes the court order to the suspect's Internet Service Provider*. Larger ISPs have their own "packet sniffers" that can collect the information without the installation of Carnivore. Those who do not are ordered to install it. The FBI may even order larger ISPs to install Carnivore, if their investigation has requirements that the ISP's packet sniffer cannot meet. (For example, the FBI may find that the ISP's sniffer would gather too much information and violate the privacy of innocent third parties.) Since ISPs have expressed the concern that incompatibilities between Carnivore and their system software might lead to disruption of service, the FBI tries to work with the software that the ISPs already have, using Carnivore only as a last resort.

4. *FBI agents then configure Carnivore according to the specifications of the court order*. The documents section of this case shows some of the screens offered by Carnivore as well as configuration options. Carnivore must be set up to ensure that the data collection conforms to court specifications. According to the FBI, these configuration possibilities separate Carnivore from other packet filters. They argue that proper configuration of Carnivore guarantees that the FBI collects only those communications to which it has legal access. Given all the available options, they hold that Carnivore is least likely to invade privacy or undermine other civil rights. Carnivore's critics, however, do not accept these claims.
5. *Carnivore filters the data stream emanating from the ISP to the Internet, selecting and copying only the targeted communications*. This is where it gets its name. While everything goes through its "mouth" (like its cousin, Omnivore), it only "digests" the meat, i.e., the targeted communication. It "spits out" everything else.
6. *Data collected by Carnivore is stored on a 2 G Jaz drive, sealed in a plastic bag, and carried by hand within the FBI Quantico facility to a secure storage area*. The FBI has adopted a series of procedures to restrict access to Carnivore-generated material. These procedures plus the security offered at the Quantico facility play a key role in the FBI's certification that Carnivore, of all the available surveillance options, is the least invasive. They also work to guarantee accountability. Carnivore's critics and even the independent review carried out by the Illinois Institute of Technology Research Institute find these data storage, audit, and accountability procedures to be fall somewhat short of these guarantees (ref).
7. *Other software, (Packeteer and CoolMiner) refine the data collected by Carnivore into a form that can be studied by FBI agents*. FBI agents authorized to review Carnivore data, remove it from its physical storage facility and use other components of the DragonWare software package to further refine the surveillance material. If for any reason Carnivore has collected data beyond the scope of the surveillance order, all the collected data must be thrown away. But Carnivore is programmed to prevent this from happening. If everything is working well, Carnivore should filter out all irrelevant data.

Legal Context

Carnivore must also be situated within the legal context governing surveillance in the United States. While privacy is not mentioned in the U.S. Constitution, its foundation can be established through other Constitutional provisions and from common law precedent. For example, the 4th amendment protects against unreasonable searches and seizures while the 5th amendment asserts that individuals cannot be deprived of life, liberty, or property without due process of the law. These provisions are the *Constitutional* basis for privacy. The *common law* basis can be found in cases like *Griswald vs. Connecticut* and *Roe vs. Wade.* These decisions provide precedents for "decisional privacy", i.e., the right to be left alone when making personal decisions.

Since technology has created new avenues for invading privacy, Congress and the Courts have worked together to frame investigative and surveillance activities so as to balance security and civil rights. For example, telephones, when a new technology, provided past criminals with new possibilities of communication and organization. But countervailing

technologies like wire taps were developed in response. One technology disrupts the balance, another counteracts, and finally the balance is restored through changes in the underlying social-technical system. In this case, the Omnibus Crime Control and Safe Streets Act of 1968 specified the purpose, scope, and thresholds for telephone wiretaps. (Specifically the Title III amendment set forth the framework on telephone wire taps.) Out of this act and Congressional reaction to intelligence abuses during the Nixon and Reagan administration, three key distinctions emerged:

1. Under **purpose**, legislators and courts distinguished between intelligence gathering and criminal prosecution. Intelligence gathering consists of collecting information to spot and develop defenses against possible threats to security. Criminal prosecution, since it is directed against individuals, would have to take place within a framework that guaranteed protection of the suspect's civil rights. This wall between criminal investigation and intelligence gathering was designed to limit the invasiveness of surveillance and prevent abuses of civil rights.
2. Under **content**, legislators and courts distinguish between general and specific information. General information includes who is sending and receiving messages but does not extend to the message's text or content. While sufficient for carrying out background investigation, general information is not detailed enough to serve as evidence in a criminal prosecution. Detailed or specific information provides the basis for criminal prosecution. Both the information and the method used to gather it are more invasive and thus pose a greater threat to individual rights. Pen Register and Trace and Trap procedures are used to gather general information, i.e., who is the sending the message and who is receiving it. Wire Taps gather the entire content or text of the message, so they are used to provide specific information.
3. Courts and legislators have also distinguished different levels of justification or **thresholds.** This distinction follows from purpose and content. Surveillance designed to provide full *content* for the *purpose* of gathering evidence for a criminal prosecution has a high threshold; because it is more invasive, the countervailing arguments must be stronger. Surveillance designed to provide only general, background information (*content*) for the *purpose* of intelligence gathering would have the lowest threshold. Low thresholds require showing relevance to some ongoing intelligence concern while high thresholds require a demonstration of probable cause, i.e., that a crime has been or is about to be committed.

These three issues (content, purpose, and threshold) provide a framework for balancing surveillance needs against civil rights. The Carnivore case raises the problem of how to extend this framework to computers. The Foreign Intelligence Surveillance Act of 1986 does this by drawing analogies between the two. Packet filters that capture the entire content of Internet communication provide the online analogue for a full telephone wire tap; the purpose, content, and threshold framework for wiretaps can be applied here. Packet sniffers or filters provide the analogue to telephone trap and traces plus pen register; they filter the Internet data stream to gather only the "to-from" information embedded in message headers. Continuing with the analogy, receiving permission to capture the entire content of an online message requires meeting the threshold of

probable cause, while gaining permission to filter out header information requires only that the investigator meet the lower threshold of **relevance**.

9-11 has changed all of this. Congress responded to al-Qaida terrorist attacks by passing the Patriot Act which has had three impacts on Carnivore. First, the Patriot Act breaks down the wall between intelligence gathering and criminal prosecution. To prevent future terrorist incidents, Congress felt it necessary that security agencies such as the CIA and NSA be able to share information and collaborate on overlapping investigations. However, intelligence agencies have lower thresholds to meet than criminal investigative agencies like the FBI. This is why the Church Commission which studied the covert activities of the CIA in the 1970's decided to separate intelligence and criminal investigations; their intention was to prevent further civil rights abuses brought about by intelligence agency covert activities (ref). Allowing the FBI to share information captured by Carnivore with intelligence agencies undermines the effectiveness of the procedures the FBI employs to prevent Carnivore use from violating civil rights. (This includes limiting the persons who have access to Carnivore-generated information.)

Second, the Patriot Act lowers the thresholds required for surveillance by expanding the range of activities whose justification only requires showing relevance. This makes it easier to carry out Carnivore-instrumented surveillances and allows these to be more invasive (ref).

Finally, the Patriot Act contains what are popularly called "sneak and peek" provisions that allow for searches and seizures without prior notification. The presence of the targeted individual at searches and seizures has traditionally served as a check against abuses of civil rights by law enforcement officials by making sure that the search is restricted to that allowed by the court order. Sneak and peek provisions remove this check by delaying notification until after the search or seizure. In some circumstances, searches and seizures are allowed without any notification at all. Carnivore is designed to work secretly; FBI and court procedures must be added to make sure that information is collected in a way that does not violate civil rights. By removing these external checks, the Patriot Act substantially expands the zone of secrecy and deepens the invasiveness of Carnivore searches (ref).

These three components of the Patriot act (lowering thresholds, breaking down the wall between investigation and prosecution, and adding sneak and peek provisions) serve to expand and amplify the power of Carnivore. For this reason, the concerns of Civil Rights Groups summarized in the next section become all the more important.

Opposition to Carnivore

Carnivore became public by accident after it had been in operation for two years. A lawyer representing an internet service provider (ISP) resisting the installation of Carnivore onto its system let the cat out of the bag while testifying before a Congressional Subcommittee in April 2000 (ref). Shortly after this a *Wall Street Journal* article brought Carnivore to widespread public attention (ref). Civil Rights Groups, including the American Civil Liberties Union and the Electronic Privacy Information

Center, reacted immediately. Under the Freedom of Information Act, EPIC requested the release of all FBI Carnivore-related documents. When the FBI resisted, EPIC obtained a court order that gave the FBI until August 16, 2000 to set forth a time table for releasing the documents. Eventually the FBI complied and many of these documents can be found at EPIC's website and in the supporting documents section of this analysis. But, as a quick glance will verify, the FBI has blacked out many parts of the released documents. Moreover, many of the technical disagreements concerning whether Carnivore will capture communications from innocent third parties, arise from the fact that Carnivore's source code has not been released and therefore cannot be independently studied for programming errors. The FBI has withheld Carnivore's source code to prevent criminals and terrorists from having the opportunity to study it, identify its weaknesses, and develop countermeasures.

Opposition to Carnivore falls generally into two camps: those who see it as a threat to civil rights and those who see it as a threat to a free Internet. Those concerned about civil liberties see several problems:

1. Can Carnivore's information gathering power tempt the FBI to go on fishing expeditions? Precedents for this fear clearly exist. For example, former FBI Director, J. Edgar Hoover, who bore a personal grudge against Martin Luther King, illegally bugged King's private conversations and tapped his phone calls. He then gave the captured information to King's political opponents exhorting them to use it to discredit King. Carnivore could instrument such fishing expeditions. Do further technical and procedural checks exist to prevent this?

2. From a technical standpoint, can Carnivore filter out all the communication that falls outside the scope of legitimate surveillance? Carnivore opponents argue that filtering out irrelevant information requires some surveillance of the very information to be filtered. Marc Rotenberg of EPIC puts this well when debating Carnivore with FBI spokesperson, Larry Parkinson, on PBS's NewsHour which was broadcast on July 24, 2000 (before 9-11):

> But the filtering technique that you're describing requires identifying search terms[.] [For example], Larry Parkinson may be one e-mail address. Maybe you have pseudonyms. I imagine a good investigator would include the likely pseudonyms for the target. Those require some human determination, what terms you're going to use as you [are] filtering message traffic. I find it very difficult to believe that you've been able to construct a filtering technique that extracts only the court-authorized information. That's a very difficult problem, even for experts in artificial intelligence.

Technically speaking, can a packet filter be developed that captures only the targeted information and nothing else?

3. Has the FBI implemented sufficient procedural checks to ensure that only qualified and authorized agents use Carnivore and review its information? When the Church

Commission recommended that a wall be placed between criminal and intelligence investigators to prevent the two from sharing information, this wall provided substantial assurance that information gained by one party could not be leaked to the other in a way that circumvents legal thresholds for surveillance. The procedures used by the FBI to prevent the acquisition of Carnivore-captured information by unauthorized persons (separating the capture computer from the control computer, storing the information on a Jaz drive, and locking it in a black box at the Quantico facility) can be undermined by over zealous agents. Furthermore, the Patriot Act breaks down the wall between intelligence and criminal investigation to promote the sharing of information gathered by both these parties since it is widely believed that 9-11 could have been prevented had all the agencies collecting information on al-Qaida been able to share this with one another. But pushing the balance toward security leaves privacy vulnerable. Can the FBI be trusted under this new environment to use Carnivore in a way that does not violate civil rights of both the innocent and the suspected?

4. Is Carnivore programming sufficiently free of errors to guarantee that it would operate according to specifications and intentions? Since the FBI was not forthcoming on where Carnivore came from (Was it developed out of commercially available software?) and since they refused to release its source code, civil rights groups argue that programming errors or shortcuts could lead to unintentional but damaging violations of civil rights. In fact, this concern has been documented in a chilling incident revealed in a memo that has been included in the documents section of this case. According to FBI documents obtained by EPIC, Carnivore captured at once too much and too little information. An FBI agent noticed that Carnivore had captured communications outside the authorized parameters of the court order. Established procedure required throwing out all the data captured. Later, it was discovered that the target of surveillance was al-Qaida. Thus, the information thrown out probably included al-Qaida activities prior to 9-11. The memo characterizes this as an ongoing problem with Carnivore.

5. Judicial oversight may fail to check Carnivore abuses because of a weakening of surveillance thresholds. In the same broadcast from the PBS NewsHour cited above, FBI spokesman presents a typical Carnivore surveillance scenario:

> Well, let's take the example of a terrorist incident, for instance. If we had evidence that some terrorist group was communicating, let's say two terrorist members were communicating with each other,…we might go to the ISP, the Internet service provider, and ask them to do a number of things. One thing might be simply to identify the to and from, who are the messages being sent to and from. Or if we could restrict it to who the message is simply going out or coming in. Or we could seek content if we wanted to see content. We wouldn't do that without going to court and getting a court order. And in order to get a court order, we have to make certain threshold showings. And we never would deploy Carnivore or any other electronic surveillance device without going to the court, getting a court order, and being supervised by the court. Now, Carnivore is rarely used, it's a surgical tool that is used occasionally….

But FBI spokesman, Larry Parkinson, made this statement before 9-11. The Patriot Act has lowered surveillance thresholds in many cases from probable cause to relevance. Moreover, it has expanded the range of content that can be captured in surveillance activities and has reduced requirements for judicial oversight. As the Patriot Act removes external checks to surveillance abuse, more and more responsibility for safeguarding civil rights must be located in Carnivore software architecture and FBI procedures. Since new versions of Carnivore and post Patriot Act FBI procedures operate without outside supervision, citizens' interest groups and civil rights organizations have good reason to be concerned.

Carnivore has features that allow it to be configured around court orders that have been carefully tailored to meet a legal framework that balances security and civil rights. So a strong argument can be constructed that it protects civil rights in the pre 9-11 socio-technical system, although this argument has been weakened by at least one documented instance of a Carnivore failure. But the socio-technical system for which Carnivore was originally designed no longer exists. In the post-9-11 world, many of the safeguards that have prevented Carnivore-instrumented abuses in the past have been removed. This has fueled the concerns of Citizens' Interest Groups like the ACLU and EPIC.

Those contributing to www.stopcarnivore.org raise similar objections plus the additional concern that Carnivore threatens the continuation of a free and decentralized Internet. Four concerns detailed in this website are quoted below:

1. **It's Unconstitutional:**
   The Constitution is largely a document of limits—limits on the way sin which Government may interfere with our lives. The Bill of Rights (the first ten Amendments to the Constitution) is a short list of specific aspects of our lives which Government may not interfere. The 4th Amendment clearly prohibits such sweeping invasions of privacy and property as Carnivore commits.
2. **It Threatens Freedom and The Internet:**
   The best thing about the Internet, the thing which has allowed it to prosper as much as it has, is lack of centralized control. And while there are those who would use this lack of control to their criminal advantage, it would be a far worse consequence to give up the "chaos" in favor of stringent control. All of the wondrous possibilities that the Internet offers us come at the price of it having no central control or governing body. To impose that type of control will be at the expense of the freedoms which have made the Internet what it is today. For 30 years, Government control stifled and suppressed the growth of the Internet. We must not allow such a fate to be reinstated.
3. **It Sets a Bad Precedent:**
   What if the FBI said they wanted to monitor all telephone calls, for information about suspected criminals? What if they wanted to intercept all postal mail, to check and see if any of it was related to any of their suspects? What if they wanted to do a "profile" of the average marijuana user, by scanning huge amounts of electronic data, and compiling the marijuana-related communications? What if they wanted keys to everyone's houses, in case they had to get inside to investigate a crime?

Use of the Carnivore system plants the seeds for all of those types of developments, and many more frightening ones.

4. **It Will Harm Innocent People:**
   The FBI can hardly be trusted to conduct their investigations with proper handling and precision, but even if they could, Carnivore will end up hurting innocent people. The amount of guesswork involved in a sweeping search like the type Carnivore does insures that many "dead ends" and "bad leads" will be pursued. What this means is that the FBI will inevitably end up investigating (including search, seizure, intimidation, prosecution, etc) innocent people. The use of a mass-level tool like Carnivore simply insures that these will occur more frequently, and at a more widespread level.

In short, www.stopcarnivore.org sees Carnivore as one of a set of computer-enhanced tools designed to remove freedom on the Internet.

Government Response to Carnivore Opposition
The U.S. Department of Justice responded to Carnivore opposition by funding an independent study into Carnivore. The Illinois Institute of Technology Research Institute was awarded a grant of $175,000 to answer four questions:

1. Does Carnivore provide investigators with all, but only the information it is designed and set to provide in accordance with a given court order?
2. Does Carnivore introduce any new, material risks of operational or security impairment to an Internet Service Provider's (ISP's) network?
3. Does Carnivore introduce any risks of unauthorized acquisition, whether intentional or unintentional, of electronic communication information by: (1) FBI personnel or (2) persons other than FBI personnel?
4. Do Carnivore and the FBI provide protections, including audit functions and operational procedures or practices, which are commensurate with the level of the risks it produces?

IITRI gave a cautious but generally supportive assessment of Carnivore and its surrounding operational procedures. They acknowledged that Carnivore (and the associated programs, CoolMiner and Packeteer) had embedded programming errors and needed debugging, concerns which have led Citizens' Interest Groups to ask the FBI to release its source code for careful debugging. More pointedly, they cited a lack of auditing and accountability procedures needed to ensure that Carnivore would be used responsibly. They concluded that the FBI should continue to use Carnivore since it was more privacy-preserving than the available alternatives including the packet sniffers used by the ISPs. But they recommended more oversight combined with continued improvements.

The IITRI report sparked opposition from both Citizens Interest Groups and software development experts. EPIC expressed doubts that Carnivore would provide "only the information it is designed and set to provide". They also reiterated their demand that the FBI release Carnivore's source code.

A group of software programming experts criticized the IITRI report for not giving careful enough consideration to how Carnivore interacted with ISP software. The concern that Carnivore would negatively impact expensive IPS software was behind EarthLink's reluctance to install it onto their system. Moreover, this panel criticized Carnivore for capturing only incriminating communications while filtering out communications that exonerated suspects. Many of the experts on this panel came from universities which were asked by the US Department of Justice to submit proposals for the Carnivore study but declined to do so. Two reasons stood out from those offered by these institutions: (1) that the due date for the final report did not allow proper time for a thorough study of Carnivore and (2) that they were concerned that the FBI would not be willing to release enough information to carry out a thorough investigation.

9-11 undermined much of this opposition by providing Congress the motive to readjust the balance between security and privacy heavily favoring security. Suddenly privacy concerns about Carnivore seemed unimportant. Two days after 9-11, AOL agreed to help the FBI carry out surveillance related to hunting down the terrorists. EarthLink publicly announced that it would cooperate with the FBI in whatever way to join in on the War on Terrorism. U.S. Congressman, Representative Armey, who before 9-11 was an outspoken critic of Carnivore, now saw it as necessary in the fight against terrorism. The Department of Justice, now under Bush Administration, wrote the Patriot Act which was quickly approved by Congress. The Patriot Act consists of a series of legal measures designed to expand the range of legal surveillance and break down the wall between intelligence gathering and criminal prosecution. As was said above, the Patriot Act changed the context of Carnivore by (1) lowering legal thresholds for obtaining court permission to carry out surveillance, (2) breaking down the wall between intelligence and criminal investigations established in the 1970's by the Church Commission to protect privacy, and (3) implementing "sneak and peek" provisions to allow searches and seizures without prior notification. Proponents of the Act were motivated by the conviction that 9-11 could have been avoided had the different agencies collecting information on al-Qaida been able to share information and cooperate more fully. In fact, 9-11 was attributed to a break down in U.S. intelligence gathering efforts due primarily to a lack of cooperation between different agencies such as the CIA, NSA and FBI.

Pre 9-11 concerns about civil rights abuses had disappeared in lieu of heightened concerned about beefing up homeland security. While a few members of Congress expressed concerns about some of the more invasive provisions of the Patriot Act, proponents silenced them by placing time limits on the most controversial measures. These "sunset provisions" are due to expire in 2005 after a five-year probationary period. In July 2005 when Congress began debate on renewing the sunset provisions, critics lamented that the DoJ had withheld information on the uses of the Patriot Act for reasons of national and domestic security. Nevertheless, permanent enactment of these provisions seems likely given continued concern about terrorist covert activities.

Carnivore is still being used and the Patriot Act has extended the range and depth of information that it can legally capture. Continued opposition led the FBI to change its name to the less inflammatory, DCS-2000.

Time Line

1791	Adoption of the 4th, 5th, and 14th amendments of the U.S. Constitution (reasonable search and seizure and due process)
1968	Omnibus Crime Control and Safe Streets Act (Title III amendment on wire taps)
1986	Foreign Intelligence Surveillance Act (18 USC 3121-3124 for Pen register and trace-trap thresholds)
Aug 1995	Russia passes SORM law (Operative-investigative activity) "giving state right to control postal, telegraph and other communications, wiretap phones and intercept information from technical communication channels"
July 1997	Downing of TWA Flight 800. FBI lobbies "for additional surveillance powers plus a ban on strong cryptography"
1997	Appropriations to FBI for development of Omnivore
1999	Appropriations for development of Carnivore
July 2000	Russia passes order 130 requiring common carriers to install "operative-investigative measures" at their own expense to aid in surveillance
August 2000	Russian Ministry of Communications drops charges against Bayard Slavia Communications
Feb 4, 2000	U.S. Central District Court issues order requiring EarthLink to allow the installation of Carnivore
April 2000	Robert Corn-Revere reveals Carnivore's existence in testimony before Congress. Corn-Revere represented an ISP resisting Carnivore installation.
July 11, 2000	Wall Street Journal article confirms and further publicizes Carnivore's existence and use by FBI
July 12, 2000	EPIC files request under FOIA for release of FBI's documents on Carnivore
Aug 2, 2000	Judge gives FBI 10 days to provide timetable for release of Carnivore Documents
Aug 12, 2000	FBI commits to first release of Carnivore documents in 45 days. Claims that there are 3000 pages of documents to review
Aug 23, 2000	DoJ issues call for proposals for "Independent Technical Review of the Carnivore System
Sept 26, 2000	DoJ announces that IITRI has been selected to conduct independent review of Carnivore system. (MIT, Stanford, Purdue, & UCSD declined to submit because of proposal constraints)
Nov 17, 2000	Draft Technical Report due
Dec 8, 2000	Final Technical Report due

Dec 2000	Citizen Interest Groups react to IITRI report on Carnivore claiming that FBI should release source code so it can be open sourced to remove bugs.
Dec 2000	Expert Panel criticizes IITRI report. More investigation needed on interaction of Carnivore with IPS software. Neglected risk that Carnivore might filter out communication that shows innocence of target.
Feb 2001	FBI changes name of Carnivore to DCS-1000
June 11, 2001	Kyllo V. United States (99-8508) 533 U.S. 27 (2001) Rejects evidence obtained by using a thermal imagining device to detect the growing of marijuana inside a private residence without a search warrant
September 11, 2001	Al Queda Terrorists attack U.S. targets, using the Internet to recruit, raise funds, and coordinate actions
September 13, 2001	AOL agrees to allow FBI to install Carnivore to check email records of suspected hijackers. EarthLink, in spite of concerns about compatibility of Carnivore with its software, promises to cooperate with FBI investigation.
October 26, 2001	Patriot Act passed. Act lowers thresholds on surveillance, breaks down wall between intelligence and criminal surveillance, and institutes sneak and peak measures
July 2005	Patriot Act Sunset Provisions come due. Bush administration campaigns to make measures permanent. Civil Liberties groups claim that there were abuses.

Patriot Act: Select Provisions

SEC. 206. ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting `, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,' after `specified person'.

SEC. 213. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.

Section 3103a of title 18, United States Code, is amended--

(1) by inserting `(a) IN GENERAL- ' before `In addition'; and
(2) by adding at the end the following:

(b) DELAY- With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if--

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);
(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and
(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.'.

SEC. 214. PEN REGISTER AND TRAP AND TRACE AUTHORITY UNDER FISA.

(a) APPLICATIONS AND ORDERS- Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended--

(1) in subsection (a)(1), by striking `for any investigation to gather foreign intelligence information or information concerning international terrorism' and inserting `for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution';
(2) by amending subsection (c)(2) to read as follows:
(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.';
(3) by striking subsection (c)(3); and
(4) by amending subsection (d)(2)(A) to read as follows:
(A) shall specify--
(i) the identity, if known, of the person who is the subject of the investigation;
(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.'.

(b) AUTHORIZATION DURING EMERGENCIES- Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended--

(1) in subsection (a), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'; and
(2) in subsection (b)(1), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'.

SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

(1) by inserting `or trap and trace device' after `pen register';
(2) by inserting `, routing, addressing,' after `dialing'; and
(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

(a) IN GENERAL-

(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.
(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--
(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
(iv) any information which has been collected by the device.
To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.
(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).'.
(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--
(A) in subparagraph (A)--
(i) by inserting `or other facility' after `telephone line'; and
(ii) by inserting before the semicolon at the end `or applied'; and
(B) by striking subparagraph (C) and inserting the following:
(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and'.
(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--
(A) by inserting `or other facility' after `the line'; and
(B) by striking `, or who has been ordered by the court' and inserting `or applied, or who is obligated by the order'.

(c) DEFINITIONS-

(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:
(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or'.
(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--
(A) by striking `electronic or other impulses' and all that follows through `is attached' and inserting `dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication'; and
(B) by inserting `or process' after `device' each place it appears.
(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended--

(A) by striking `of an instrument' and all that follows through the semicolon and inserting or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;'; and
(B) by inserting `or process' after `a device'.
(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended--
(A) by striking `and'; and
(B) by inserting `, and `contents' after `electronic communication service'.
(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by striking `the terms of'.
(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting `or other facility' after `the appropriate line'.

SEC. 218. FOREIGN INTELLIGENCE INFORMATION.

Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking `the purpose' and inserting `a significant purpose'.

Independent Technical Review of the Carnivore System: Final Report

Carnivore Executive Summary

9 Pages

Socio-technical System

This section will explore the socio-technical system (STS) of Carnivore. An STS is a conceptual tool used to understand the entire system within which any particular computing system is embedded. Ethical issues hardly ever arise about disembodied, abstract systems. Instead, they arise when a computing system comes into contract with the real world, socio-technical context. Chapter 11 (Social Frameworks) provides a detailed overview of socio-technical systems, including how they embody value. Chapter 2 (Problem Specification) discusses how to carry out a socio-technical analysis and how to spot problems that arise because of value mismatches within STSs and between STSs and computing systems.

The components of a socio-technical system can include hardware, software, physical surroundings, people, roles, procedures, laws & regulations, and data & data structures. Thus a STS can be quite complex. In this section, you will discover some of the more important pieces of the STS surrounding the Carnivore case.

Hardware
Carnivore hardware components

- COTS (Commercial Off The Shelf) Box
- Two gigabyte Jaz Drive
- No TCO/IP Stack
- Network Isolation Device
- Black Box or Black Metal File Cabinet
- Two off the shelf PCs: collection computer and control computer

The material captured in the collection computer is stored on the 2G Jaz drive. The Jaz drive is then removed, sealed in a plastic bag and taken to a physical storage facility where it is put in a black box or black metal file cabinet. Later, the Jaz drive is placed in the control computer where the captured data is reconstituted into a form that can be analyzed by specially trained and approved FBI agents. These 2 PCs, the storage facilities at Quantico, and typical ISP hardware (wires, routers, and servers) form the hardware of the Carnivore STS

Software
The Carnivore software package is called DragonWare and has three parts: Carnivore or the packet filter, Packeteer which refines the captured data into higher levels, and CoolMiner which displays the captured content in a Web browser. The FBI provided the IITRI with the source code for Carnivore 1.3.4. However, they did not provide the source code for Carnivore II which was in the alpha testing phase at the time of the IIT study. Carnivore critics have hypothesized that Carnivore was developed out of commercial packet filters such as those used by internet service providers to filter out spam. For example some have suggested that the FBI built Carnivore out of AG Group´s EtherPeek. If this is the case, there may be problems with the programming brought about by shortcuts to meet strict deadlines (ref). The IITRI final report provides a more technical description of the Carnivore software package (Page ix):

Carnivore software has four components: (1) a driver derived from sample C source code provided with WinDis 32, a product of Printing Communications Associates implements preliminary filtering of IP packets; (2) an application program interface (API); (3) a dynamic link library (DLL) written in C++ provides additional filtering and data management; and (4) an executable program written in Visual Basic provides a graphical user interface. Functionality is placed in the driver whenever possible to enhance performance. Evolution of the source code between v1.3.4 and v2.0 clearly indicates that all process will eventually take place in the driver. The DLL provides entry points for functions such as INITIALIZE, START, STOP, and SHUTDOWN. The user interface is divided into basic…and advanced…screens. The basic screen allows an operator to start and stop collection, view collection statistics, and segment the output file. The advanced screen allows the operator to define and redefine the filter parameters that control what Carnivore collects.

People, Groups & Roles

1. *FBI*: The FBI developed Carnivore for the purpose of carrying out electronic surveillance into criminal activity. But Carnivore has features that allow it to be used for a wide variety of surveillance activity from gathering general evidence for background investigations to capturing detailed information to serve as evidence in a criminal prosecution. For criminal prosecution, FBI agents must show that the evidence is gathered in conformity with Rule 901 of Federal Rules of Evidence. This helps show that the methods used to obtain evidence have not violated the civil rights of those who stand accused as well as innocent third parties. Carnivore offers features that document the legitimate and non-invasive gathering of evidence. FBI agents also provide arguments to obtain court permission to carry out surveillance. Agents must adhere strictly to the structure of the court orders or subpoenas in carrying out their investigations. Going beyond court allowed parameters can lead to agents being dismissed or even prosecuted. Finally, the FBI is concerned about its reputation and public image. When the Wall Street Journal publicized FBI use of Carnivore, they suffered immediate adverse public reaction. Spokespersons for the agency emphasized the features of Carnivore designed to prevent invasive surveillance. They also justified Carnivore in the face of the increasing reliance of criminals and terrorists on the Internet for carrying out their activities. Carnivore has been presented as a defensive weapon designed to protect innocent citizens from harm perpetrated by criminals and terrorists.
2. *Intelligence agencies and the Department of Homeland Security*: The responsibilities and roles of intelligence agencies and the FBI have been kept separate out of concern for citizen civil rights. This wall between intelligence activities and criminal prosecution was put into place to prevent the FBI and intelligence agencies such as the NSA and the CIA from sharing information with one another. Intelligence agencies have substantially different uses for electronic surveillance. Their concern is to monitor the activities of terrorists and terrorist organizations to protect U.S. citizens from a repeat of 9-11 so it is easier for them to gain court permission. In a word, security agencies are less accountable for guaranteeing that their activities will

not abuse or violate civil rights. The wall between the FBI and intelligence agencies exists to prevent the FBI from circumventing civil rights. Information gained by intelligence under less stringent thresholds should not be made available to the FBI who is subject to stricter thresholds. This difference in role between intelligence agencies and the FBI also points to different stakes. The NSA and CIA are obliged with protecting homeland security. Failure to do so, manifested in calamities like terrorist attacks can lead to a loss of public faith in their effectiveness which, in turn, leads to investigation and restructuring.

3. U.S. citizens: U.S. citizens have two fundamentally different constellations of rights at stake. First, they have the right to security, that is, the right to be protected against occurrences like 9-11. To do their job, intelligence agencies collect information on the activities of suspected criminals, spies, terrorists and other wrong doers. Since their focus is preventive, they are given broader latitude in the scope of information they can gather and the techniques they can use to gather it. But guaranteeing homeland security can come into conflict with safeguarding other civil rights such as privacy and due process. Citizens need security to go about their daily business. But citizen social, economic, and political life requires the protection of rights such as privacy and due process. Organizations such as the FBI and CIA exist to provide for security. Countervailing organizations like the American Civil Liberties Union and the Electronic Privacy Information Center have arisen to protect this other set of liberties. Thus citizen interests lie in a social, political, and legal framework that balances security with civil rights such as privacy and due process. The emergence of the Patriot Act, which readjusts this balance towards security and away from privacy and due process, shows how delicate this balance is, and how it must be continually maintained.
4. Internet Service Providers: ISPs serve as portals through which paying customers enter into the Internet. Their survival requires that they keep their customers satisfied by providing continuing quality service and protecting the confidentiality of information about these customers. But ISPs play a key role in the surveillance activities carried out by intelligence agencies and the FBI. While they are required to obey court orders requiring that they allow the FBI to install Carnivore, they have a legitimate interest in ensuring that Carnivore is compatible with their software. EarthLink claimed that incompatibilities between their software and Carnivore could lead to expensive disruption of service. The IITRI report provided general assurances that Carnivore would not lead to systems breakdowns. Nevertheless, critics of the IITRI report claimed that the compatibility of Carnivore and ISP software had not been studied carefully enough.
5. Citizen's Interest Groups: The ACLU and EPIC are citizen interest groups who have played a key role in the Carnivore. The ACLU is concerned with the general protection of civil rights. They provide legal representation for citizens whose civil rights have been violated. EPIC is focused on the issue of privacy. In Carnivore, they used the Freedom of Information Act to force the FBI to release Carnivore documents. Citizen's interest groups provide collective support for individual civil rights. But they also need to maintain a balanced relation between the groups they oppose, especially government agencies. On the one hand, they need to strike an adversarial relation designed to ferret out information of possible rights abuses by

government agencies. On the other hand, they need to maintain some basis for cooperation and collaboration.

Procedures
A fuller description of these procedures is provided in the Historical Narrative above.
1. *The FBI receives court permission* (in the form of a court order to an Internet Service Provider) *to conduct surveillance on a suspected individual*.
2. *The strictness of the threshold requirements the FBI must meet depends on the information sought and the purpose of the surveillance*.
3. *The FBI takes the court order to the suspect's Internet Service Provider*.
4. *FBI agents then configure Carnivore according to the specifications of the court order*.
5. *Carnivore filters the data stream emanating from the ISP to the Internet, selecting and copying only the targeted communications*.
6. *Data collected by Carnivore is stored on a 2 G Jaz drive, sealed in a plastic bag, and carried by hand within the FBI Quantico facility to a secure storage area*.
7. *Other software, (Packeteer and CoolMiner) refine the data collected by Carnivore into a form that can be studied by FBI agents*.

Laws & Regulations
Much of the Carnivore legal context can be understood by looking at how US Wiretap law has been analogically extended to include electronic communication. The interrelated legal framework consisting of content, purpose, and threshold is discussed in detail above. Below in this section is a general discussion of the issues that arise in US Wiretap law.

US Wiretap law

Probable cause and wiretaps. A wiretap allows the law enforcement agency to listen in on conversations on a telephone line. Under standard wiretap law, in order to obtain a wiretap order, highly placed federal officials have to make the request and federal judges have to approve it. The official has to make the case to the judge that there is "probable cause" to believe a crime has been committed or that one is about to be committed, that regular attempts to resolve the problem have failed. The order needs to be quite specific about for whom, where, and how long the tap will be. Judges are also given the imperative to "minimize the interception of communication of data." Within 90 days after termination, targets must be notified. There are limited exceptions to these rules for emergency situations. There are less restrictions for taping foreign nationals in the USA.

Pen register, trap and trace and electronic communication. Less authorization is required for a "pen register" which is just a tap on the numbers that are called or a "trap and trace" a tap on the calls placed to a particular telephone. This is analogous to just looking at to and from headers of email.

Patriot Act. Under section 215 of the Patriot act, the probable cause requirements are loosened to "to justify an investigation for a non-citizen, it is necessary that the

investigation be for the purpose of obtaining foreign intelligence information. If the investigation concerns a citizen, the standards are higher: the purpose of the investigation must be protection against international terrorism or clandestine intelligence activities" (from www.usdoj.gov. google for Patriot Act Section 215). This search cannot be reported to the target (or anyone). Under the "sneak and peek" provisions, notification of a search is no longer required. Pen register and trap and trace authority now only have to certify that they are "relevant to an investigation." There is a balanced article on Patriot on Slate.com.

The legal trail forming the context of Carnivore can be summarized in the following table:

Carnivore Legal Trail

Year	Law, Statute, Amendment, or Regulation
Nov 3, 1791	Adoption of the 4th, and 5th amendments to the U.S. Constitution (reasonable search and seizure and due process)
July 28, 1868	14th Amendment to the U.S. Constitution: Due Process
1968	Omnibus Crime Control and Safe Streets Act (Title III amendment on wire taps)
196?	Griswald vs. Connecticut
197?	Roe vs. Wade
1974	Privacy Act
1986	Foreign Intelligence Surveillance Act (18 USC 3121-3124 for Pen register and trace-trap thresholds)
1986	Computer Fraud and Abuse
1994	CALEA
1998	Roving Wiretap
2001	Patriot Act Passed
2005	Patriot Act Sunset Provisions come due

Data and Data Structures
The data and data structures at play in Carnivore can be analyzed on two levels.

First, because Carnivore is a packet filter, the primary data with which it is concerned are the packets of information that pass over the internet. Carnivore consists of algorithms designed to capture specifically targeted data. The filtering works on the basis of the information that is embedded in each packet, ranging from the to and from information to the actual content.

Second, on a higher level, the data collected by Carnivore consists of online conversations and activities carried out by individuals who are either suspected of criminal activities or are the subject of intelligence-gathering operations. The content captured depends on the court order. This, in turn, depends on the purpose of the investigation (intelligence or criminal), the threshold of proof required for court approval (relevance to an intelligence operation or probable cause), and the purpose of the investigation (intelligence background investigation or gathering evidence for a criminal trial).

Data flowing into the Internet stream through an ISP portal is filtered by Carnivore and stored on a Jaz drive connected to a collection computer. This information is then removed physically and the Jaz drive is placed into a control computer where Packeteer reconstructs the raw data into higher level IP packets and CoolMiner displays it in a Web browser.

Carnivore Exercises: Version 2 (Started September 17, 2005)

Annotated Bibliography

1. Read carefully the Carnivore report commissioned by the U.S. Department of Justice and carried out by the Illinois Institute of Technology. Its official title is, "*Independent Technical Review of the Carnivore System: Final Report,"* which was prepared by the Illinois Institute of Technology Research Institute. The full report can be found on the website of the Electronic Privacy Information Center whose web address is www.epic.org/privacy/carnivore/carniv_final.pdf . This report provides sample screens, detailed information about Carnivore's architecture, and a good summary of Carnivore's strengths and weaknesses. While it does not give the last word on Carnivore, it does represent a good beginning.

2. The passage by the U.S. Congress of the Patriot Act greatly changes the STS in which Carnivore operates. Hence, one must carefully study the impact of the Patriot Act on electronic surveillance. The EPIC website is a good place to start. It provides a report that introduces the controversial provisions of the Act.

3. "*A Guide to the Patriot Act*," by Dahlia Lithwick and Julia Turner provides an excellent follow up to the EPIC discussion. This article discusses key provisions and their concrete impacts. It can be found online in Slate Magazine at http://slate.msn.com. The posting date is September 8, 2003.

4. Larry Lessig. *The Future of Ideas*
Larry Lessig. *Code and Other Laws of Cyberspace*
These books discuss packet filters, Internet architecture, P2P software, and encryption technologies. In *Code*, Lessig argues that values are integrated into Cyberspace through *software* (code), *norms*, *laws*, and the *market*. Chapter two of this book makes a similar claim for socio-technical systems. Values are integrated into computing technologies and the underlying socio-technical system through hardware, software, physical surroundings, people/groups/roles, procedures, laws, data & data structures.

5. Kevin Bowyer and colleagues at the University of Notre Dame's Department of Computer Science and Engineering have carried out extensive research on Biometrics. Bowyer describes a course developed at Notre Dame that studies the ethical implications of Biometrics. His paper, "*An Elective Course in Biometrics and Privacy*," has been published in the **Proceedings of the 34th annual conference of the ASEE/IEEE Frontiers in Education Frontiers in Education** and can be found at http://fie.engrng.pitt.edu/fie2004/index.htm. Other publications on biometrics can be found at Bowyer's website, http://www.cse.nd.edu/~kwb/.

6. *The Good Computing Manuscript,* Chapters 2 and 11, provide information on how to do **Good Computing Reports**. Chapter 2 discusses the different parts of the project: scoping, interviewing, constructing surveys and questionnaires, triangulation, and preparing your executive summary. Chapter 11 discusses the view on technology that

underlies the report. Also read the chapter on *Carnivore* which includes an historical narrative, time line, legal trail, ethical reflections, historical documents, and an STS description. The chapter on *Educational Laptops* summarizes presentations given by students in Computer Ethics 2004-5 in the ethical reflections section. This section also analyses problems that stem from value mismatches and unanticipated consequences.

7. Spinello & Tavani. Readings in CyberEthics, editions 1 & 2. Jones and Bartlett. 2001, 2004. Spinello and Tavani provide an excellent anthology of readings in CyberEthics that are divided into chapters on many of the intermediate moral concepts in good computing: privacy, intellectual property, security and free speech.

8. Deborah Johnson. Computer Ethics, 3rd Edition. Prentice Hall. 2000. This has long been the most popular and most useful textbook in computer ethics. Johnson includes chapter-length introductions to the intermediate moral concepts. Each of these chapters concludes with helpful bibliographical information. Good Computing makes use of two of her theses: (1) problems in computer ethics are new species of old genera and (2) computers "instrument" or magnify human action. For example, while threats to privacy are nothing new, Carnivore raises the specter of a new a more invasive threat to privacy. Packet filtering software instruments human action in that it provides the means of sifting through the vast data streams of the Internet to capture specific bits of information.

9. Electronic Privacy Information Center www.epic.org. The Report on Carnivore prepared by the *Illinois Institute of Technology Research Institute* can be found on the EPIC website. EPIC also displays Carnivore documents obtained from the FBI through the Freedom Of Information Act (FOIA). (Note that the FBI has blacked out substantial portions of these documents before releasing them to the public.) Besides archives on Carnivore and the Patriot Act, EPIC also provides free downloads of privacy protection software. Carnivore groups may find it useful to examine this software.

10. "A Guide to the Patriot Act," by Dahlia Lithwick and Julia Turner. http://slate.msn,com Posted September 8, 2003. Lithwick and Turner provide a careful, comprehensive, and user friendly guide to the highlights of the Patriot Act. This may be the most useful introduction you will find.

Exercise 1: Carnivore Requirements Analysis

Groups one and two are consultant teams hired by the FBI to help develop monitoring systems. Group one will carry out a requirements analysis focusing on Citizens' Interest Groups (CIGs) and Internet/Online Service Providers. Group Two will identify the requirements of the FBI and the Department of Homeland Security.

A requirements analysis begins by identifying key stakeholders and specifying their needs. Then it describes what a software design that fulfills these needs would look like. This analysis overlaps with problem specification. For example, a requirements analysis specifies value mismatches between monitoring technology (e.g., Carnivore) and different socio-technical systems (e.g., a free Internet). It also examines how monitoring technology exacerbates value conflicts within a socio-technical system. For example, it might show how the enhanced surveillance instrumented by Carnivore exacerbates the conflict between the FBI's commitment to protect privacy and its mandate to prevent terrorist attacks on U.S. citizens. This analysis also identifies unexpected or remote consequences that lead to harms such as the unintentional capturing of information about innocent parties due to errors in Carnivore software development or configuration.

An effective requirements analysis identifies and understands specific user needs. What are the needs of the FBI, Citizens' Interest Groups, and Internet Portals, Service Providers, and Online Service Providers? Could these be met by packet filtering software such as Carnivore? Should the FBI consider different technologies like biometrics? Can software be designed for packet filters that can be configured to balance conflicting privacy and security needs? Will the requirements analysis recommend finding or developing new, less invasive technologies?

Group One:
Group one will carry out a requirements analysis centering on the **FBI**, a criminal investigative/prosecution agency, and the **Department of Homeland Security**, an intelligence agency. The intermediate moral concepts in good computing will help highlight special needs or requirements. These concepts include security/safety, privacy, equity, free speech, and property. For example, the concept of *security*/safety highlights the FBI´s mandate to prevent terrorist attacks. But *privacy* brings out the conflicting requirement that it work to protect the privacy of U.S. citizens. In what situations do these requirements conflict with one another? What kind of software could be developed to balance and reconcile these conflicting needs?

A glance at the FBI's website shows that 9-11 has changed agency priorities. Hence, this requirements analysis should include a discussion of the impact of 9-11 and the Patriot Act. What influence has the Patriot Act had on FBI concern for privacy and security? 9-11 also led to the creation of the Department of Homeland Security and the reclassification of previously independent agencies such as FEMA. Homeland Security has three mandates: (1) prevent terrorist attacks within the U.S., (2) reduce U.S. vulnerability to terrorist, and (3) minimize damage from potential attacks and natural disasters. How consistent are these needs with one another? Have these directives

created new value mismatches? What are the unexpected consequences that have emerged from the creation of the Department of Homeland Security and the reclassification of subordinate agencies like FEMA?

Group Two:

Group Two will carry out a requirements analysis that concentrates on two different groups:

1. Internet Portals (Yahoo), Internet Service Providers (EarthLink), and Online Service Providers (AOL). These groups are key players in Carnivore-driven surveillance. What are their needs? What would software responding to these needs look like? (Note that one concern shared by these groups centers on the compatibility of Carnivore with their own system software. Can they run Carnivore without disruption of service?)
2. Citizens' Interest Groups like the Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU). These groups provide citizens with information on potential civil rights abuses, often aiding victims of civil rights abuses in obtaining effective legal defense. A glance at the EPIC website identifies the following goals: (1) focus public attention on emerging civil liberties issues, (2) protect privacy, freedom of expression and constitutional values in the information age, (3) maintain an active website, and (4) work in support of several Non Government Organization (NGO) Coalitions who are also committed to civil liberties issues.

To help identify these users' requirements, focus on the intermediate moral concepts: safety/security, privacy, freedom of speech, property, and equity. What are the requirements of these stakeholders in relation to these concepts? (Do customers of Online Service Providers like AOL have privacy needs? Do they have security concerns? Do these needs conflict with one another? Can we envision software designs that minimize or even eliminate these conflicts?)

It is important to distinguish between Internet Service Providers (EarthLink), Online Service Providers (AOL), and Internet Portals such as Yahoo or Google. Their needs may be quite different. For example, while EarthLink was concerned that Carnivore would be incompatible with their software this was not a problem for AOL.

Both groups one and two should give special consideration to pre and post 9-11 requirements. Prior to 9-11, a clear framework existed under which surveillance could be conducted. Criminal investigation was clearly distinguished from intelligence gathering, probable cause (the criminal investigation threshold) from relevance (the intelligence gathering threshold), and search targets were notified prior to search or seizure. The Patriot Act passed after 9-11 changed all of this by producing the following changes:

- Addition of Terrorism and Computer Crimes as Predicate Offences
- Expanded Dissemination of Information Obtained in Criminal Investigation

- Sneak and Peak Provisions
- Extended Scope of Subpoenas for Records of Electronic Communication
- Lowered Standards for Foreign Intelligence Surveillance
- Roving Wiretaps
- Liberalized Use of Pen Register/Trap and Trace Devices
- Section 215 of the Patriot Act brings the Internet communication within the scope of legally bounded surveillance
- Sunset Provisions: Due to expire in 2005 unless re-approved by Congress

Exercise 2: The FBI Green Team

This exercise requires two groups. Both respond to the mandate that the FBI has to upgrade information technology infrastructure. Group one will examine biometrics technology as an effective upgrade while Group two will look at non-biometrics. Each will choose two technologies; two biometrics systems and two non-biometrics systems. Upon choosing the technologies, each group will compare their two technologies to each other and to Carnivore in terms of constituent needs and requirements, the intermediate moral concepts, and potential value mismatches.

Group Three
Group Three consist of consultants hired by the FBI to help them respond to the mandate to upgrade information technology infrastructure. Carnivore represents one of the baselines against which upgrades will be measured.

The first task consists of choosing two biometrics technologies. Examples include pattern recognition technologies such as facial recognition or optical scans. (For a futuristic vision of a world dominated by biometrics and other high tech surveillance technologies see the movie, Minority Report.) Kevin Bowyer, director of the University of Notre Dame Department of Computer Science, provides several articles at his website to help you get started. (The web address can be found in the annotated bibliography at the beginning of this section.)

After choosing two biometrics technologies, compare, evaluate, and rank these in relation to each other and to Carnivore. Be sure to identify stakeholders and respond to their stakes/needs. To help identify stakes and needs, examine each stakeholder in relation to the intermediate moral concepts we have studied this semester: safety/security, privacy, free speech, property, and freedom of expression. Also consider feasibility factors such as time for implementation, technical viability, cost, and general fitting into the social, historical, legal and political aspects of the underlying socio-technical system.

Finally, using the methodology we have developed through problem specification, check for value mismatches. These include (1) mismatches between the biometrics technology and the underlying STS, (2) mismatches within the STS exacerbated by the integration of the biometrics technology, and (3) unanticipated long term results of the integration of the technology.

Group Four:
Group Four will also respond to the mandate to the FBI to upgrade information technology infrastructure. The difference is the scope of this investigation: it will encompass all but biometrics. Group Four will choose two non-biometrics technologies and identify the stakeholders who will experience impacts from their use. As with Group Three, Four will compare, evaluate, and rank these tools in relation to one another and to Carnivore.

To prime the pump, what are the possible targets of criminal and terrorist activity that these technologies should protect? A preliminary list would include the following:

> ftp, P2P, telnet, gopher, voice over IP, email, web-based communication, etc

Possible tools to select and evaluate would include the following:

> Packet filters, decryption devices, general monitoring systems, search engines (to zero in on terrorist sites), and automatic translators (to translate terrorist sites prepared in different languages)

Group four begins by choosing two non-biometric technologies. Examples include decryption devices and terrorist search engines.

The Online NewsHour archive has a program aired August 2, 2005 that provides a good discussion of how terrorists exploit online resources. This can be found at www.pbs.org/newshour. The Washington Post also published a useful article of how terrorists operate online. Its title is "Terrorists Turn to the Web as Base of Operations" by Steve Coll and Susan B. Glasser. This article first appeared Sunday, August 7, 2005. Looking at how terrorists operate online can help in identifying and conceptualizing software countermeasures to these activities.

After choosing two non-biometrics technologies, compare, evaluate, and rank these in relation to each other and to Carnivore. Be sure to identify stakeholders and respond to their stakes/needs. To help identify stakes and needs, examine each stakeholder in relation to the intermediate moral concepts we have studied this semester: safety/security, privacy, free speech, property, and freedom of expression. Also consider feasibility factors such as time for implementation, technical viability, cost, and general fitting into the social, historical, legal and political aspects of the underlying socio-technical system.

Finally, using the methodology we have developed through problem specification, check for value mismatches. These include (1) mismatches between the non-biometrics technologies and the underlying STS, (2) mismatches within the STS exacerbated by the integration of the non-biometrics technology, and (3) unanticipated long term results of the integration of these technologies.

Exercise Three: FBI Blue Team

Group Five
This group has been commissioned by the FBI to play the role of technologically savvy criminals and terrorists who are developing countermeasures to the technology upgrades being developed by the FBI. This exercise can be divided into four stages.

1. Scope possible technologies that could be used to monitor online behavior. Examples include biometrics, decryption devices, packet filters, thermal imaging, search engines, and data mining. Commercial and freeware versions exist of at least some of these

technologies. The driving standard here is to identify technologies that could be used to monitor criminal and terrorist activities.

2. Choose two for further, in-depth study. Criteria for selection could be the availability of commercial or freeware versions, likelihood of use by the FBI or intelligence agencies, the potential effectiveness of this software, or the possibility of developing countermeasures.

3. Develop countermeasures to the monitoring technologies chosen. Playing the role of criminals and terrorists, how would the Blue Team go about circumventing these technologies? The Washington Post article mentioned above provides several strategies currently employed by terrorists that could help start the brainstorming process. Dead drops, concealing messages in a sea of Spam, encryption, and developing redundant web sites are just a few of these strategies.

4. The intermediate moral concepts studied this semester provide a double-edged sword for the Blue Team. Take security, for example. What measures could be adopted to promote the security of a terrorist group? Then, turning to the other edge, what measures could terrorists take to undermine security measures implemented to thwart their efforts. How do terrorist groups maintain the privacy of their online communications while invading the privacy of other groups, such as the FBI? And so forth.

A note to all groups:

These exercises deliberately overlap. The goal is to synthesize them into an overall comprehensive view of the Carnivore case. While you should be aware of and respond to what the other groups are doing, you should also make an effort to go in different and new directions. The differences and overlaps that will emerge in the presentation cycle will provide your group considerable input that you can build into the written report you will turn in later. Feel free to collaborate, interact, and respond. Avoid duplicating and imitating.

Packet Filters (Sniffers)

Name	Description
Omnivore	Captures all traffic to and from a specific IP address. Carnivore's predecessor
Carnivore	Proponents claim that it is a robust system that won't capture data from innocent people. But others have questioned its robustness by saying that developers could have taken programming short cuts that could lead to problems. (Robert Graham, Carnivore, FAQ
Altivore	Offered as an alternative to Carnivore for ISP's concerned about the harmful impact of Carnivore on their server systems. Network ICE has made the source code available. Added feature: packet reassembly. (In Carnivore this is done by CoolMiner)
Network ICE: Packet Logging	Personal Firewall
AG Group's EtherPeek	Possible commercial package upon which FBI built Carnivore
TCPDUMP	Used by Graham to construct a simple packet filter or sniffer

STS—Carnivore

Hardware & Software	Physical Surroundings	People, Roles, Institutions	Procedures	Laws & Regulations	Data / Data Structures
Hardware: PC Computer	FBI Quantico Headquarters (Physical security measures)	FBI Department of Justice	Obtaining a court order or search warrant for wire tap	U.S. Constitution: 4th and 5th amendments	Internet Data Stream: Packets
$80,000 intercept system at Quantico requiring modem	Facilities for storing and accessing information collected by Carnivore	Courts carrying out judicial oversight	Obtaining permission for pen register or trace-trap	Omnibus Crime Control and Safe Streets Act (1968)	Data captured by Carnivore
Jaz Drive	Surroundings at IITRI where Carnivore was tested	Civil Liberties Groups	Notifying target of search and seizure	Title III amendments	Data filtered by Carnivore
Internet components: computer network		Cyber terrorists, Cyber criminals, hackers, disgruntled employees	Configuring Carnivore	Foreign Intelligence Surveillance Act (1986)	Data stored in Jaz Drive
Software: ISP packet sniffers		Innocent third parties in cyber space	Gathering Intelligence	Patriot Act: Sections 206, 213, 214, 216, & 218	Data reconstructed into higher level packets by Packeteer
DragonWare: Carnivore Packeteer CoolMiner		Internet Service Providers	Compiling evidence for criminal prosecution		Data displayed by CoolMiner in Web Browser

People Groups and Roles

Stakeholder	Role	Stake	Stake Mismatches
FBI	Promoting domestic security via intelligence gathering and criminal prosecution	Public Trust Congressional Funding	Zealous pursuit of security could lead to violations of privacy
Bad Guys	Using computers and Internet to break law and harm targeted individuals and organizations	Remaining Free Achieving political objectives Receiving benefits	Actions could lead to centralized control of Internet Could also undermine individual rights (Patriot Act)
Internet Service Providers	Providing access to Internet as well as other services for paying customers	Maintaining customer base, trust, and privacy Avoiding penalties for not carrying out court orders and subpoenas	Following court orders and subpoenas could lead ISPs to violate privacy and lose trust
U.S. Citizens	Autonomous individuals with certain natural and legal rights that must be respected	Rights and Goods such as Security, Privacy, Due Process	Enhancing security may come at the expense of privacy and due process
Citizens of Foreign Countries	Individuals, autonomous in a moral sense, whose rights are unclear in the U.S.	Dignity which includes natural rights such as privacy and security	Conflicting loyalties
Courts	Oversee intelligence and criminal surveillance	Could lose public trust if unable or unwilling to protect and balance citizen's rights	Difficulties in balancing security with other rights such as due process and privacy
U.S. Congress	Oversight on activities of DoJ Consult with executive branch on judicial appointments Legislate to protect rights	Reputation Political appointment (lose election) Integrity (Compromising within the limits of integrity)	Balancing security with privacy and due process

People Groups and Roles

Stakeholder	Stake	Stake	Stake Mismatches
U.S. Department of justice	Enforcing the law and exercising oversight over surveillance of U.S. citizens	Successfully prosecute criminals Balance security with privacy and due process Protect the Constitutional and legal rights of citizens	Security frequently conflicts with due process and privacy Zealous prosecution can lead to undermining civil rights of suspects
IITRI	Conduct independent investigation of Carnivore as specified in tasks and questions	Reputation and Research Integrity Public and Academic Trust	Difficulty of carrying out an independent investigation given constraints of call for proposal (short timeframe and FBI withholding information)
EPIC	Identify, disseminate and respond to threats to the privacy of U.S. Citizens	Maintaining credibility and trust Organizational integrity	Need to maintain a productive but adversarial relation with the government
ACLU	Identify, disseminate and respond to threats to the civil liberties of U.S. Citizens	Maintaining credibility and trust Organizational integrity	Need to maintain a productive but adversarial relation with the government
stopcarnivore.org	Stop Carnivore and publicize the possibility of Carnivore instrumented abuses of rights	Integrity & credibility Responding to threats to human and civil rights Maintaining a free Internet	Adversarial relation with FBI may threaten credibility and ability to get crucial information
Private Software Development Firms (Network ICE, AG Group)	Develop software that responds to consumer needs, is secure, reliable, and profitable	Maintaining credibility, trust, and integrity	Classified Carnivore information makes it difficult to benchmark and improve packet filters Criminals will develop counter measures if Carnivore information and source code become public
Intelligence Agencies (Central Intelligence Agency and National Security Agency)	Collect intelligence relevant to cover international terrorist activities	Carry out surveillance without violating fundamental ethical and civil rights	Difficulty of developing effective defenses against terrorism without violating due process and privacy rights