

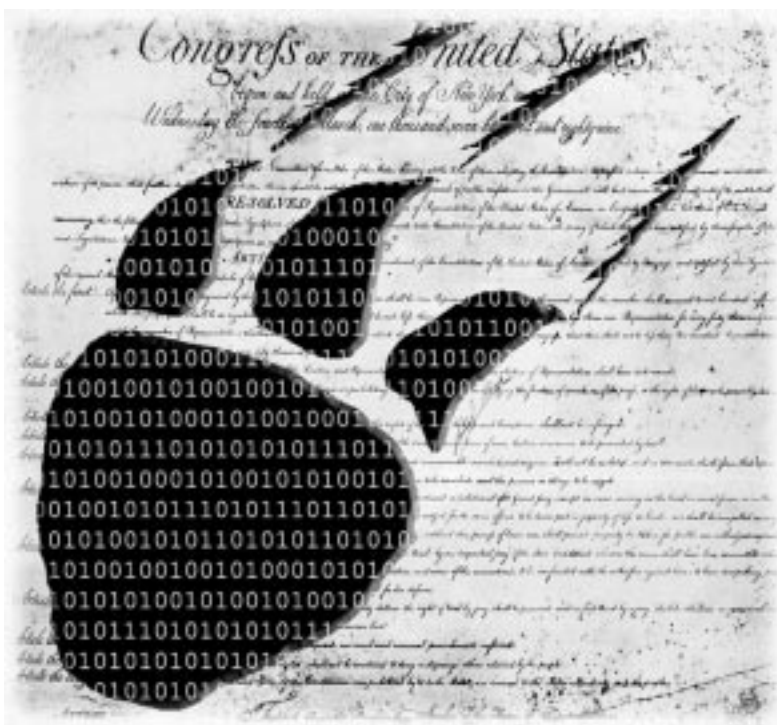
# Carnivore and Controversy

*Catherine Shaw*

**T**echnology law is increasingly becoming an area of concern and controversy as the world grows more dependent on technology for communication, information sharing, decision making, and daily living. With this new technological frontier comes the responsibility to guard the rights of its users and formulate new policy to answer the new questions brought about by change. These questions deal with how much protection of privacy users of the Internet can expect under the Fourth Amendment. Internet-related technologies are foremost in the developing areas of technology. These innovations are creating a new reality for users to anonymously conduct activities of expression, exploration, and education over the Internet.

Over 300 million people access the Internet daily for e-mail, stock quotes, advertising, research, and many other general-viewing purposes. Internet users are taking advantage of the benefits of being connected and have been pushing the limits of the digital network. They increasingly want to make more sophisticated use of the Internet as a processing tool for database applications, software downloads, and media streaming, all of which result in an extremely busy online community in which both sensitive and personal information is often shared.

The nature of communication over the World Wide Web is such that anonymity is preserved and indeed a protected. Users of the Internet presume that their e-mail will not be scanned or read without due process. Communication over the Internet is similar to voice communications, and it is possible to design security and surveillance regulation that treats e-mail as such. E-mail correspondence is both spontaneous and comes with implicit trust between online associates that the pen name (user name, handle, screen name) used in communication is a valid identity. Based on similarities



between electronic communication and voice communication, it does not seem far-fetched to ask that rules regulating voice wiretaps be used as a baseline to draw regulations for electronic communication. There exist extensive guidelines in 18 U.S.C. 2510-2522 that stipulate the rules for wiretapping in criminal investigations. It is proposed in this paper that congress adopt the same level of respect of privacy when constructing regulatory principles dealing with Internet surveillance.

## Problem Definition

The latest in Internet surveillance, the wiretap tool created by the FBI known as Carnivore, has justifiably caused much public concern over the general subject of the Internet and the Fourth Amendment. According to the Fourth Amendment:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, support by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Citizens are afforded freedom and protection against unreasonable searches. It is imperative that our notions of privacy and personal security continue to make sense in the face of increased Internet use. Before the rise of the Internet, people stored all sensitive information in their homes. Now, however, if a third party wants access to information stored on a computer, an invasion of privacy is simply a point and a click away. How much control should the FBI be given to monitor a person's personal electronic communication?

Carnivore has raised some serious questions regarding online privacy. When installed, it implements a combination of software and hardware capable of sniffing all electronic packets that are sent to and from an Internet Service Provider (ISP). Carnivore is capable of monitoring everything from e-mails to web requests and responses, logins, instant messages, and chats. Privacy advocates argue that the use of Carnivore is unconstitutional under the Fourth Amendment because Carnivore initially scans all the e-mails at the given ISP in order to track and collect targeted mail. They further argue that Carnivore has a potential to be misused by the FBI. According to

the FBI, they have used Carnivore in at least twenty-five criminal and national security investigations; the FBI maintains that the system is legal and is not a breach of the Fourth Amendment.

Policy that adequately protects Fourth Amendment rights should be the ultimate goal of all parties that have input on this matter. Emphasis should be placed on utilizing the existing policy in 18 U.S.C. 2510-2522 to construct regulations for Internet surveillance. Implementation of that policy can be twofold: modify Carnivore's source code to limit operations and/or legislate regulations on proper use of Carnivore.

## Legislative History

A quick discussion of the earliest interpretations of the Supreme Court on the relevance of the Fourth Amendment to wiretaps is presented in the cases *Olmstead v. United States* (1928) and *Katz v. United States* (1967). Title III of the Omnibus Crime Control and Safe Streets Act (1968, 18 U.S.C. 2510-2520) went into effect to establish procedures for court-ordered wiretapping and bugging. The statutory scheme was quickly outdated because of the advances in technology and Supreme Court hearings of *U.S. v. Miller* (1976). This prompted the enactment of the Electronic Communications Privacy Act of 1986 (ECPA). A large hole in the scope and attention to detail in ECPA is in the distinction between stored e-mail and real-time electronic communications. This hole has been exploited by the FBI such as in *Steve Jackson Games, Inc. v. U.S. Secret Service* (1994). The most recent cases concerning Internet privacy and anonymity are *McIntyre v. Ohio Elections Commission* (1995) and *ACLU v. Johnson* (1998). The next sections will establish the current direction of Internet surveillance regulation and will describe how Carnivore fits into this scheme.

## Civil Liberties

Conducted secretly in a transparent fashion to the user, electronic surveillance is unlike most searches in the physical world. There is no apparent awareness of being observed, and the persons under scrutiny have no sign of the implementation of tools such as Carnivore. Since this sort of investigative surveillance monitors both innocent and incriminating communications, there is reason to call forth the Fourth Amendment and

question whether or not electronic surveillance is the type of general search warrant that the Fourth Amendment protects citizens against.

Statistical data suggests that the use of electronic surveillance has become increasingly resented by the public and more leniently implemented by the FBI. During the first five-year period for which the Wiretap Report (published annually by the Administrative Office of the U.S. Courts) was available, less than half of intercepted communication was innocent. For the most recent five-year period, only one-fifth of the intercepted communications was incriminating, meaning that four-fifths of the intercepted communication was innocent. For every instance of federal or state use of electronic surveillance, there are on average 1,600 innocent communications intercepted.

This loss of personal privacy is alarming considering the rate at which people are using the Internet. Indeed, the lack of privacy over the Internet is a reason that many do not participate in e-commerce opportunities and do not utilize the Internet for sensitive communication. These users are among the respondents to the Department of Justice's yearly inquiry on wiretapping. Approximately three-fourths of the population are against the use of Internet surveillance because it undermines the trust between a government and its people.

### **Olmstead v. United States (1928) and Katz v. United States (1967)**

The first landmark court case in this area was *Olmstead v. United States* (227 U.S. 438) in 1928. The case involved a conspiracy to violate the National Prohibition Act by importing and selling liquor. *Olmstead* was the leader of a business to commit these black market acts. The information that led to his arrest and the determination of his guilty intent to distribute was found by officials who intercepted phone calls outside *Olmstead's* residence. The issue at hand was whether or not the use of private phone conversations equals a violation of the Fourth and Fifth Amendments. In a close vote of 5 to 4 the Supreme Court decided that the use of wiretap was not in violation of the amendments. Chief Justice Taft wrote the majority opinion and took a strict interpretation of the Fourth Amendment: There was no search or seizure of physical property. There was no entry of the accused, and by

the invention of the telephone and its use for the purpose of communicating over a distance, the language of the amendment cannot be extended to include telephone wires.

This decision was reversed in 1967 in the case of *Katz v. United States*, which established a doctrine of "reasonable expectation of privacy." *Katz* was convicted of sending wagering information across state lines using a telephone booth that was bugged by the government. A search warrant had not been obtained. Even though a telephone booth was a public place, the search was ruled unconstitutional because a person could reasonably expect privacy there. "...It is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable..." The Supreme Court reversed the conviction, stating:

"The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."

In reply to the government's argument that there had been no physical violation of property, the Supreme Court concluded, "that the underpinnings of *Olmstead* [and *Goldman*] have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."

*Katz v. United States* also established a perquisite for probable cause. Searches conducted without a warrant were to be deemed unlawful.

"Even electronic surveillance substantially contemporaneous with an individual's arrest could hardly be deemed an 'incident' of that arrest. [Footnote] Nor could the use of electronic surveillance without prior authorization be justified on grounds of 'hot pursuit.' [Footnote] And, of course, the very nature of electronic surveillance precludes its use pursuant to the suspect's consent." [389 U.S. 356-58]

The Court held that a phone conversation could not be intercepted without a warrant.

### **Omnibus Crime Control and Safe Streets Act (1968)**

After *Katz v. United States*, congress recognized the need to formalize safeguards to protect individual rights to privacy. It established procedures for court-ordered wiretapping with the Omnibus Crime Control and Safe Streets Act in

1968. Important points of this act were:

- 1) Electronic communications were to be bugged only for specific serious crimes.
- 2) Internet surveillance could only be implemented when there is a court order showing probable cause of crime.
- 3) Internet surveillance was likely to be used as a last resort.
- 4) Precaution would be taken to minimize capture of innocent conversation.

These provisions were codified in 18 U.S.C. 2510-2520.

### **Data Stored by Third Parties— Smith v. Maryland (1979) and U.S. v. Miller (1976)**

Contents of general electronic communications were protected in the Omnibus Crime Control and Safe Streets Act (1968). However, the act did not anticipate the storage and use of stored electronic communications for investigative purposes by third parties. In *Smith v. Maryland* (442 U.S. 735) the Court held that the Fourth Amendment does not protect the privacy of numbers dialed on the phone, because phone companies routinely record numbers dialed for business purposes and a person has no reason to expect privacy from the numbers they call. This notion of reasonable expectation was used in *U.S. v. Miller* (425 U.S. 435) in which the Court held that people do not have a “reasonable expectation of privacy” recognized under the Fourth Amendment that pertains to financial records maintained by their banks (about the individuals) during the normal course of business. Legislators were not ready to deal with the new technology that allowed simple storage of sensitive information to distant third parties.

### **Stored Communications and Real-Time Communications— ECPA (1986) and Steve Jackson Games, Inc. v. U.S. Secret Service (1994)**

E-mail was formally addressed in the Electronic Communications Privacy Act of 1986. The ECPA is not as protective of e-mails as the Title III is to voice communications. The reasoning for this is that real-time interception is to be given greater protection than retrieval of past communications logs. To this end, the government has exploited the Act. The Supreme Court

has been less protective of this stored information. This can be problematic because the saved e-mails of an individual are likely significant to the recipient than the e-mail that he or she deletes upon reading.

Under ECPA, real-time interception of e-mail messages is protected more stringently than the acquisition of the same message from a “provider of electronic communications service” after it has been stored. Real-time interception requires a court order based on probable cause of crime and is used as a last resort of investigation as required by the Omnibus Crime Control and Safe Streets Act. Once a message has been stored, access is gained under the section of the U.S. Code that deals with requirements for government access. 18 U.S.C. 2703 has less stringent prerequisites for capture of stored data. In other words, just by waiting for that instant in which a message is delivered and “stored” by a mail handler, the FBI can avoid the statutory requirement for minimization procedures (minimize the amount of innocent material), the last resort requirement, and the requirement of a court order (a warrant issued by a magistrate is good enough). Congress enacted ECPA to specifically address the concerns of the public on e-mail privacy and inadvertently created a loophole for the FBI to take advantage of.

In *Steve Jackson Games, Inc. v. U.S. Secret Service* (36 F.3d 457, 5th Circuit 1995), the Supreme Court found that court orders are rarely sought to intercept e-mail as it is sent. Instead, the government waits until the e-mail has been stored and pursues a warrant under 18 U.S.C. 2703 (and not 18 U.S.C. 2510-2522). The Court tolerated use of the loophole in the ECPA regulation in this ruling.

### **Privacy and Anonymity on the Internet: McIntyre v. Ohio Elections Commission (1995) and ACLU v. Johnson (1998)**

In the years after *Steve Jackson Games, Inc. v. U.S. Secret Service*, two major cases were logged in the realm of Internet privacy and anonymity. In *McIntyre v. Ohio Elections Commission* (514 U.S. 334) it was held that Ohio Code’s prohibition of the distribution of anonymous campaign literature abridges the freedom of speech in violation of the First Amendment. Joseph McIntyre distributed leaflets purporting to express the views

of “Concerned Parents and Taxpayers” opposing a proposed school tax levy and was fined for violation of Ohio Code, which prohibits the distribution of campaign literature that does not contain the name and address of the person or campaign official issuing the literature. The finding was reversed by the Court of Common Pleas, but the Ohio Court of Appeals reinstated the fine. In affirming, the State Supreme Court held that the burdens 3599.09(A) (Ohio Code) imposed on voters’ First Amendment rights were “reasonable” and “nondiscriminatory,” and therefore valid. The majority writes: (a) The freedom to publish anonymously is protected by the First Amendment, and (b) extends beyond the literary realm to the advocacy of political causes.”

As the Supreme Court championed our rights to speak anonymously, it would follow that the Court would continue to protect the right to free speech over the Internet.

Two years later in *ACLU v. Johnson* (4 F. Supp.2d 1029) the District Court of New Mexico found that a “New Provision (as it was called in the brief)” signed by the Governor of New Mexico, Gary Johnson, was in violation of the right to communicate and access information anonymously under the First and Fourteenth Amendments of the U. S. Constitution. The Provision was set in place to censor from minors indecent material on the Internet. The Court found that the restrictions in the provision were too broad and infringed on the rights of individuals to express and share thoughts anonymously.

## **Carnivore from the Viewpoints of Pertinent Parties: FBI Presentation of Carnivore**

The contents of the FBI’s defense of Carnivore its web site on the Carnivore Diagnostic Tool pages. The ability of law enforcement agents to conduct lawful electronic surveillance represents one of the most important capabilities for obtaining evidence of criminal acts. Electronic surveillance has been used in the past thirteen years to secure the convictions of over 25,000 felons. Recently, the FBI has utilized Carnivore more frequently because criminals increasingly use the Internet to chat with each other and, chillingly, to talk to their victims. The Carnivore program allows a trained user to intercept and collect communications with “surgical” ability.

An ISP (Internet Service Provider) has a high-

speed connection directly to the Internet. It “sub-lets” access to the general population, who cannot afford or maintain such connections on their own. Users connect to the ISP, which in turn connects them to the Internet through its own connection. Most ISPs lack the ability to discriminate among all the packets (literally, packages of information sent over the network) of communication that come and go routed through its hub. Consequently, the FBI has developed Carnivore as a tool to help filter for communications that can be lawfully intercepted and ones that cannot. For example: if a court order allows only for the interception of one type of communication (e-mail) but not, for example, shopping transactions—then Carnivore can be configured to intercept only those e-mails. There is no mention on the FBI Carnivore Site of the other related techniques the FBI uses to obtain, for example stored e-mail.

The FBI cites its compliance with the Communications Assistance for Law Enforcement Act (CALEA) as evidence of its diligence of compliance with relevant code and regulations in use of Carnivore. However, the ACLU uses CALEA as an example of how the FBI seeks to undermine the Fourth Amendment.

## **ACLU’s Objections**

The American Civil Liberties Union has been very vocal in its support of the Fourth Amendment and raised many of its concerns to congress in hearings before the House Judiciary Committee-Subcommittee on the Constitution. They are a nationwide, nonprofit, nonpartisan organization with over 275,000 members who champion the principles set forth in the Bill of Rights. They have spoken out a number of times for Civil Liberties in congressional hearings and have been vocal in the issues surrounding Carnivore. What follows is a summary of key points made in from of the House Judiciary Committee-Subcommittee on the Constitution in July of 2000.

It is clear that ISPs are willing to cooperate 100 percent with the FBI and law enforcement agencies. The ACLU, in recognition of the potential for abuse of Fourth Amendment rights in the ECPA loophole (discussed earlier in the Legislative History Section), and in recognition of how little the public and ISPs actually know about the capabilities of Carnivore, filed a

Freedom of Information Act request with the FBI. The ACLU wanted a disclosure of the source code, documentation, and operating instructions for Carnivore. The ACLU does not want to simply take the FBI's word that Carnivore will not infringe upon Fourth Amendment Rights. As a result of this inquiry, an independent review board was given the task of inspecting Carnivore.

The ACLU in its statement before the Committee also brought forth concerns about the interception of real-time communications versus stored e-mail. Wiretaps can be issued only upon showing of probable cause. E-mail can be intercepted with a court order based on probable cause issued in connection with any federal felony. The U.S.C. sections that deal with surveillance only address wiretaps and bugs, not e-mail. Once investigators can obtain access to e-mail under federal law in the ECPA, a search warrant based on probable cause issued by a federal magistrate (as opposed to a court order) is all that is needed to gain access to e-mail which has been stored for less than 180 days. By simply waiting for communication to be stored, the prerequisites of a court order and the corresponding judicial oversight can be skipped over. For messages stored for over 180 days, access can be granted much easier, needing only to establish "relevance," a much lesser threshold than "probable cause."

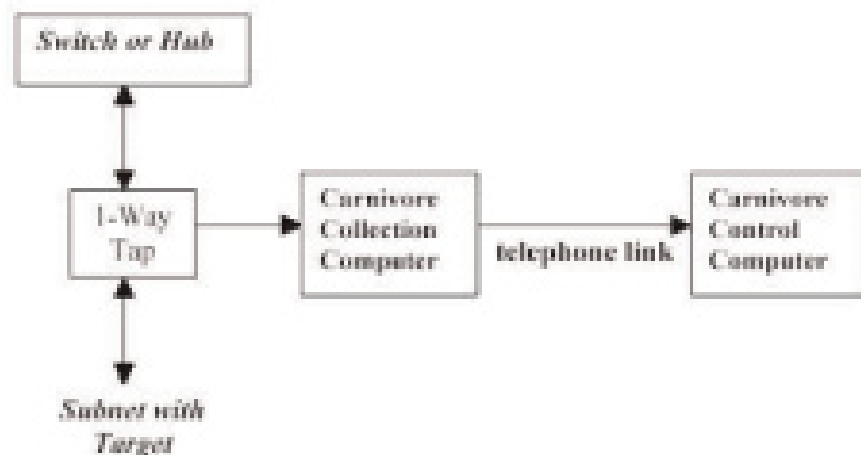
The ACLU points out that FBI history of pushing the envelope in terms of casting an increasingly wide net for Internet surveillance. In 1994, congress passed CALEA, which in effect struck a deal between the FBI and the new generation of digital networks. In return for the

requirement that the new networks be formed to be surveillance ready, the FBI promised not to force service providers to provide the FBI with surveillance capabilities (the FBI reasoning that there would be enough willing service providers to comply with surveillance needs). In retrospect, CALEA has been characterized as a power grab by the FBI. While the new digital networks complied with the standards set for the industry, the FBI has consistently pushed for have new surveillance features installed that did not exist in 1994. Some of these demands include that cellular phone providers create systems that give law enforcement officials capability to use the systems for tracking purposes, that Internet telephony providers turn over communications when asked (even when investigators only have a pen register, tap, or trace order), and other questionably invasive orders. The ACLU used CALAE as proof that the FBI should not be trusted to act as its own regulator.

### Illinois Institute of Technology's Review (ILTRI)

As a result of the application with the Freedom of Information Act, the Department of Justice formed an independent review board to examine the FBI-provided source code. ILTRI's scope of evaluation included how Carnivore is to be applied as well as its technical capabilities. ILTRI was asked to report on whether or not Carnivore could provide investigators with only the information that it is designed to and be set to provide in accordance with a court order; whether Carnivore introduces any new, material risks of operational or security impairment of

Figure 1



an ISP's network; whether the system risks unauthorized acquisition of electronic communication information by FBI; and whether Carnivore provides protections, including explicit procedures for audit and operational practices.

Their methods fell into four mostly independent tests, which involved evaluations of system architecture, limitations built into the source code, and lab simulations. To summarize its architecture, the Carnivore system consists of four main parts: (1) a one-way tap into an Ethernet stream of data; (2) a computer to filter and store collected data; (3) other computers to control collection and examination of data; and (4) telephone line links to the collecting computer. (See Figure 1.)

When the collection computer is placed at an ISP, it receives all packets that go through the ISP that match filters configured in Carnivore. The one-way tap into the communications stream ensures that Carnivore cannot alter received packets. The control computer is placed in law enforcement offices, and when linked to the collection computer via phone lines, it can be used to configure the filters, start and stop collection, and retrieve collected data on the collection computer. There are two main modes of filtering for the collection computer: pen and full-collection. In pen mode, Carnivore has access to the IP and e-mail addresses of all files transferred through FTP and HTTP sessions (FTP and HTTP are two extremely common transfer protocols). In full-collection mode, Carnivore can access all content of transactions that use FTP and HTTP protocols along with the IP and e-mail addresses of messages passed through the filter. For control computer linkage there is no user identification (all users are logged in as administrators and are anonymous to the system).

The operation of filter setting is fairly straightforward and does not provide user identification verification. In the wrong hands, Carnivore could be used to monitor the content of all electronic communication that passes through an ISP with Carnivore installed on it. This is one of the main criticisms ILTRI had of the Carnivore system. ILTRI concluded the following on the four main points it was given to examine:

- 1) If Carnivore is used correctly under a court order, it can provide users with no more information than is permitted through use of the filters.
- 2) The ISP on which Carnivore is installed does

not perform less efficiently, and running Carnivore does not pose a security risk to the network on which it is installed.

- 3) Carnivore reduces but cannot totally rid itself of risk of unauthorized obtaining of information by FBI personnel.
- 4) Carnivore does not adequately provide audit functions that match the level of risks (not enough methods of establishing accountability for actions taken using Carnivore)

ILTRI's other conclusions dealt with configuration and what Carnivore is incapable of doing. As already mentioned, since Carnivore has an easy-to-understand configuration interface and no built-in checks, it can potentially be easy to foul up a configuration. In addition, Carnivore does not always recover from power failures, does not have time synchronization, and has poor physical security for collection computers. Carnivore cannot track the comings and goings of a particular ISP's customers, monitor real-time communications (like instant messages), block traffic on a network, isolate a network, or create its own packets. Due to these faults in Carnivore's makeup, Carnivore cannot be publicly released because the potential for exploitation is too great. Therefore, measures to ensure that law enforcement agents properly use Carnivore and solutions to the current flaws in Carnivore's safe use as an Internet surveillance tool must be implemented.

## Solutions

The goal of this paper is to find some way to reconcile the FBI's responsibility to protect citizens with its use of surveillance instruments to do so. In the case of Carnivore, the object is to preserve the Fourth Amendment right of protection from unreasonable search and seizure as well as the First Amendment right of freedom of expression and anonymity.

## Drivers

In order to change the course of increasingly lenient FBI regulation standards that have been allowed in courts (*Steve Jackson Games, Inc. v. U.S. Secret Service*, 1995), drivers for change must be examined. It is unacceptable for the FBI to exploit the loophole in ECPA, as the number of innocent communications collected increases proportionally to the incriminating communications. Different things affect the willingness, opportunity, and capacity for change.

Equation 1:

$$(e^*d) \text{ mod } (p-1)(q-1)=1$$

Equation 2:

$$e^*d=1+k(p-1)(q-1)$$

Equation 3:

$$(M^*e)^*d \text{ or } (M^*d)^*e$$

Equation 4:

$$M^*((p-1)(q-1)) \text{ mod } pq=1$$

The ACLU represents the public interest in its desire for change. Since the purpose of congress is to represent concerns and values of the citizens and bring into the legislative process the views, needs, and interests of their constituency, it is expected that congress provide a forum where the interests and demands of all segments of society are expressed. Willingness to learn about issues related to privacy and civil rights will always be around as long as the ACLU continues to be a proponent and informant for the public good.

There are many options for changing the current trend. Opportunities to lower the free range of the FBI to implement Internet surveillance using Carnivore have been suggested by the ILTRI and ACLU, to include many improvements to Carnivore and modifications of clauses in the ECPA, respectively. Carnivore's architecture and code can easily be modified if the designers want to create a more exacting and monitorable version of Carnivore. The capacity to change Carnivore itself definitely exists as does the capacity to amend parts of the ECPA.

ILTRI made several recommendations for strengthening Carnivore's system architecture and enhancing built-in checks in Carnivore's software. They suggest complete separation of software capable of full-content mode and pen-register mode. Total separation will reduce probability of error in filter mode. ILTRI also recommends that the following issues be fixed in Carnivore's source code: configuration of setting with limits, identification and verification for users, and audit controls. Additionally, facilities where the computers are located need more security provisions. Even with these changes, Carnivore can truly be the exact tool for the FBI to use for surveillance routines.

The ACLU has proposed that the language of ECPA be amended to better represent intent to protect civil rights. ACLU suggests that the ECPA be amended to include specific restrictions on national implementation and use of Internet surveillance. Carnivore's net of suspicion should always be cast as conservatively as possible. Other amendments to ECPA include:

- 1) Stipulations that consumers be notified when the government finds out about Internet transactions.
- 2) Requirements that statistics be kept on how often orders are issued to use Internet surveillance and what portion of captured communications lead to criminal indictment.
- 3) Specific considerations for viewing content in full-content mode filtering, ie, making sure that there is at least a probable-cause order in place.

Strengthening the ECPA will make it harder for law enforcement to tread upon individuals' privacy rights and will eliminate the loophole that currently exists for avoiding obtainment of a probable-cause order to view e-mail that has been stored and is not intercepted in real time.

If both the approaches proposed by the ACLU and ILTRI are pursued, they would not be in conflict with one another and would definitely lead to more responsible investigative behavior. In addition, there is one avenue of technological innovation that would also help solve the controversy, were it not for government regulation of that innovation: the field of encryption and decryption. Public key encryption is currently the standard used among most security-conscious users of the web. RSA (key generation technique) is the most popular version of public and private key generation, uses mathematical techniques to encode and digitally sign data. The process begins with the generation of two large, 1024-bit, primes  $p$  and  $q$ . Then you find numbers  $e$  and  $d$  such that they satisfy Equation 1 or Equation 2.

The public key is  $(e, p*q)$ . The private key is  $(d, p, q)$ . Encryption in this scheme breaks a message  $M$  in pieces such that  $M < p*q$ . Then each piece of  $M$ , is translated into Equation 3.

That part is easy. However, when a person other than the intended receiver intercepts a message encrypted under RSA, he or she must perform many operations to make sense of  $M$  because it has the property expressed in Equation 4.

Guessing the numbers  $p$  and  $q$  from  $p \cdot q$  while only knowing  $e$ , is extremely difficult and takes a lot of computing power. Prime factorization of a 1,024-bit key takes  $10^{16}$  years. The larger the prime numbers  $p$  and  $q$  are, the harder it is to find  $p$  and  $q$  from  $p \cdot q$  without knowing  $d$  (part of the private key). Hence, the larger the key bit (number of bits needed to represent the key) the harder it is to break the encryption.

It seems that through RSA key encryption of sensitive materials online, communications could be protected from Carnivore's full-content filter mode. This is a viable avenue to explore for other encryption standards with complexity and would be even harder to break. However, currently there is no practical reason to research this field because of NSA restrictions on key bit size.

## Barriers

As touched upon in the Drivers subsection, there are several barriers to the changes proposed. Some of these barriers are imposed on innovation by the National Security Agency (NSA) and some stem from among the groups whose ideas are described above. Some of these barriers are insurmountable, but others can be deconstructed and reconciled. This subsection will describe each of these situations.

The easiest type of barrier to address is that imposed by the NSA, who wants to be able to break any sort of code that can easily be used by the public. As a matter of national security, the NSA regulates use of PGP (Pretty Good Privacy), a common application available off the Internet to create keys, requiring that those who wish to download PGP establish U.S. Citizenship. To date, there is not much to be done about the fact that the NSA restricts key bit size. The keys are large enough to protect all transactions and most sensitive communications. National think tanks are researching other methods of encryption but the subject matter is classified.

Since that particular avenue for technological innovation has been blockaded, it is important to focus on the deconstructable barriers to change. One of the largest barriers to comprehensive change of policy on Internet surveillance is that the stakeholders, ACLU and ILTRI, are not working together. In fact, the ACLU denounces the research done by ILTRI. The ACLU claims that the Department of Justice "stacked the deck" when it appointed a committee to review the

FBI's Carnivore Internet surveillance system. Names of the reviewers were former White House insiders, including past members of the NSA and former employees and consultants to the departments of Defense, Justice, and Treasury. "By selecting people with extensive government ties for what is supposedly an independent review, the Executive Branch has shown once again that it cannot be trusted with carte blanche authority to conduct searches," said ACLU Associate Director Barry Steinhardt.

While the ACLU may have a point that the ILTRI's review board could have been chosen more fairly, ILTRI still made valid suggestions for changing Carnivore that should not be discounted. ILTRI's proposals seek to provide Carnivore's law enforcement officers with a more exacting program using internal checks and stronger audit functions—both of which are in line with the ultimate goal of making the FBI more responsible in its use of Internet surveillance.

## Strategy

The preservation of the public's rights to freedom of (anonymous) expression and freedom

San Mateo (HQ) Chicago Cupertino London New York Santa Monica

**DI** DIGITAL IMPACT

*Join*  
*a fellow*  
*MIT*  
*graduate*  
*at*  
**Digital Impact**

**MIT graduate, Gerardo Capiel, is a co-founder and CTO of Digital Impact.**

As a co-founder, Gerardo helped establish Digital Impact as a leading provider of integrated eMarketing solutions that enable businesses to acquire, retain and analyze their customers. Our leading-edge clients include companies such as: **Hewlett-Packard, Electronic Arts, Coach and Citibank.**

Digital Impact is headquartered in San Mateo, CA. We are a public company, strongly positioned to expand our share in an explosive growth market. If you want to work with a world-class team, please go to our website – [www.digitalimpact.com](http://www.digitalimpact.com) for our current positions.

177 Bovee Road, Suite 200, San Mateo, Ca. 94402

## References

### Documents:

1. Bill of Rights
2. ECPA—Electronic Communications Privacy Act
3. 18 U.S.C. 2510-22 Omnibus Crime Act
4. ILTRI's Review
5. Statement of Gregory T. Nojeim  
Legislative Counsel ACLU on Fourth Amendment and the Internet before the House Judiciary Committee Subcommittee on the Constitution April 6, 2000

### Cases:

1. *Olmstead v. United States* (1928)
2. *Katz v. United States* (1967)
3. *U.S. v. Miller* (1976)
4. *Steve Jackson Games, Inc. v. U.S. Secret Service* (1994)
5. *McIntyre v. Ohio Elections Commission* (1995)
6. *ACLU v. Johnson* (1998)

### Websites:

1. <http://www.aclu.org/congress/>
2. <http://www.fbi.gov/hq/lab/carnivore/carnivore.htm>
3. <http://laws.lp.findlaw.com/>

from unreasonable search and seizure are core values of our nation that must continue to be paramount as we transition into an increasingly technology reliant era. It is important that all stakeholders make a concerted effort in regulating the use of Carnivore. It is also imperative that the public's sense of security, using the tapping of phone lines as a baseline for comparison, remains the same in the realm of the Internet. For example, legislation codified in 18 U.S.C. 2210-2222 should have a mirror image in electronic communications and in ECPA. There are two main opportunities that exist to change the existing lenient standards of action for the FBI.

The first of these opportunities is the use of legislative measures to create the aforementioned sensible consistency in protection of privacy in phone communications and the communication over the Internet. Given the careful attention to Fourth Amendment rights is in the Omnibus Crime Control and Safe Streets Act (1968) and the similarities between communication over a phone line and communication over the Internet, this seems reasonable to expect. Both are spontaneous and users do not typically question the privacy of a phone call or e-mail. In order to make the ECPA (1986) more closely match 18 U.S.C. 2510-2222, it would be wise to pursue the suggestions made by the ACLU to amend ECPA.

The second strategy is to follow the recom-

mendations of the ILTRI's evaluation of Carnivore and change the system architecture and source code as suggested. The merit of these suggestions should not be questioned even though the demographics of the review board are under scrutiny. The suggestions are valid, and if implemented would result in a positive evolution of Carnivore (it would have more self-checks and audit functions).

In conclusion, it is extremely important for groups who seek to champion civil rights and basic freedoms promised in the Bill of Rights to work together to achieve common goals. Perhaps the ACLU and ILTRI can form a more neutral task force to reexamine Carnivore and reimplement testing that the review board already conducted to verify results. Both the ACLU and the review had a common goal—the scrutinize the FBI's use of Carnivore and to check the Internet surveillance scheme of faults and checks and balances in the system. Carnivore is an effective tool when used properly and can be a valuable asset to investigators. If the ACLU and ILTRI work together, they can eliminate barriers to change and through shared resources and different strategies can bolster public awareness as well as the defense of civil rights and protected freedoms. Together they might even flush out other drivers for change that have yet to be developed. ■