# Hacktivism: Securing the National Infrastructure

*Mark Milone*

The foundations of modern society—communications, power, transportation, banking, water supply, and public institutions—depend on interconnected computer systems to operate properly. Hostile groups threaten this "National Infrastructure" by exploiting the strengths and weaknesses intrinsic in its architecture. Activists who utilize networked forms of organization, doctrine, and strategy to protect civil liberties and spread democratic values in cyberspace present an invaluable resource in securing these systems. These "hacktivists," however, must be provided with the appropriate incentives and protections to encourage coordination with government actors. Facilitating this alliance will require an understanding of the relationships between technology, law, and policy in a democratic, networked society.

Modern society is increasingly dependent on networked computer systems to facilitate its critical functions. This complex architecture, the central nervous system of our "National Infrastructure," presents novel challenges to national security. Computer-savvy activists devoted to protecting human rights and spreading democratic values present an untapped resource that can provide government with the tools, strategies, and organizational design necessary to protect our National Infrastructure and counter networked crime and terrorism. To encourage participation and ensure efficacy, these hacktivists must become educated as to the National Infrastructure's importance, the limitations faced by law enforcement in attempting to monitor and secure the National Infrastructure, and when hacktivists' well-meaning actions may result in legal liability.

---

Mark G. Milone is Associate General Counsel at the New York Mercantile Exchange where he advises on matters relating to technology, intellectual property, electronic commerce, telecommunications, and privacy. Since graduating from Hofstra Law School in 1998, Mark has founded an online business <www.virtulaw.com>, taught "Computers and the Law" at Long Island University, worked in-house with a leading multimedia design agency, and was an associate at Klein, Zelman, Rothermel & Dichter, L.L.P. This article was first published in the American Bar Association's *The Business Lawyer.* Mark would like to stipulate that his remarks herein do not reflect those of the Merc. He can be reached at <milone@mindspring.com>.

*Knowledge, Technology, & Policy*, Spring 2003, Vol. 16, No. 1, pp. 75-103.

## National Infrastructure

The National Infrastructure is composed of "critical systems" which facilitate the core functions of modern society. Without a secure National Infrastructure, telecommunications, power, transportation, banking, water supply, and emergency services would cease to operate.[1] These systems share one common element: each is dependent on computer networks to organize, coordinate, and execute functions. Each system, therefore, is susceptible to the weaknesses intrinsic in the architecture of computer networks.

### *Networks*

A "network" is defined as "an intricately connected system of things or people."[2] The concept of a network has been applied in many contexts, such as the social contacts a person makes to further his or her career (i.e., "vocational networking"), the nervous systems of living creatures ("neural networks"), and the structural arrangements used in information technology (i.e., "networked computing").[3] Regardless of its function, a network is said to follow certain "laws" that are intrinsic in its structure and composition.[4] For instance, a network's efficiency and resilience from disruption will be dependent on its structure, which can be divided into at least three types or topologies[5]:

(1) The chain or line network where people, goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes (e.g., a smuggling chain).
(2) The hub, star, or wheel network, where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that central node to communicate and coordinate with each other (e.g., as in a franchise or a cartel).
(3) The all-channel or full-matrix network, in which every node is connected to every other node (e.g., collaborative networks of groups where everybody is connected to everybody else).

One can see that a full-matrix network, such as cyberspace, presents the most efficient and resilient communications architecture. Cyberspace, however, is subject to two additional principles that apply specifically to computer networks. Namely, a computer network's value increases proportionately with the storage capacity of individual nodes (i.e., computers)[6] and the number of interconnections between nodes.[7] These principals become increasingly significant as the National Infrastructure becomes more dependent on the pervasive, full-matrix network of powerful computing machines known as cyberspace.

### *Critical Systems*

Many have studied the potential effect that attacks on critical systems pose to national security. From breaking down communications systems, to initiating electrical blackouts, to undermining our financial systems, there are a number of major disruptions that could unravel our economy, diminish our quality of life, and generally destabilize the nation.[8] In some cases, such as an attack on the national air traffic control systems, these disruptions could result in widespread damage to property and infrastructure, and serious loss of life. To make matters worse, the U.S. government has been criticized for failing to adequately protect federal computer networks against criminals and terrorists.[9]

### *Netwar*

Modern networked societies are challenged by increasingly complex, diffuse, and global threats. This phenomenon has been labeled "netwar" and is described as "an emerging mode of conflict and crime at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age."[10] Netwar's organization differs from previous conflicts in that it is "networked." This means that attacks and demonstrations can take place without a centralized command structure. Metaphorically, modern conflicts can be said to more closely resemble the Eastern game of "Go" than the Western game of Chess. It has been argued that our government has yet to implement the sweeping changes necessary to combat such networked forms of attack.

### *Hacktivism*

Online activists consist of dispersed organizations—small groups and individuals who communicate, coordinate, and conduct their campaigns in an networked manner, often without a precise central command. Like netwar, the unifying element of the new activist is the use of networked forms of coordination, policy, and technology. When such activism manifests itself in the form of surreptitious computer access or the dissemination of potentially disruptive and/or subversive software, it is called "hacktivism."[11] A hacktivist, therefore, uses the same tools and techniques as a hacker,[12] but does so in order to bring attention to a larger political or social goal.[13] Regardless of the motivation behind such campaigns, many question whether hacktivism constitutes a crime.

## Cybercrime

Criminal actions that target or are facilitated through the use of computer systems are called "cybercrime."[14] Cybercrime can be divided into two categories:

1. Crimes that are "located" entirely in cyberspace; and
2. Crimes that have a physical component which are merely facilitated in cyberspace.

### *Technology & Targets*

Each computer that is connected to cyberspace is susceptible to intrusion. Most system crackers, however, take advantage of widely known vulnerabilities that result from the lack of security features included with today's most popular operating systems, browsers, and electronic mail programs.[15] The following is a brief overview of some of the common techniques used to access and/or damage computer systems computer systems.

*Unauthorized access.* System crackers typically use cyberspace to access computer systems via "ports," which act as points of entry into the network.[16] Computer systems are designed to have hundreds of ports for different types of uses, such as electronic mail, remote log-in, or telnet. Most of these ports are not in use and remain closed, and can only be opened by a system administrator. System crackers can obtain the same privileges as a system administrator on a network, known as "superuser" or "root" status, and open one or more of these ports. This is usually accomplished by taking advantage of common holes in operating systems and applications or by taking advantage of easy-to-guess passwords.[17]

*Malicious code.* Programmers may also create and distribute malicious code (also called "malware"), such as viruses,[18] Trojan horses,[19] and worms,[20] in order to cause potentially global computer damage.[21] These applications can be broken down into five component parts/phases:

1. Propagation/migration: local replication over a computer and/or network;
2. Payload: the mechanism through which malicious code causes damage or has an effect;
3. Signature: pattern with which malicious code is detected by security software;
4. Detection avoidance: the method by which malicious code attempts to hide itself; and
5. Trigger: action through which malicious code is activated.

*Distributed denial of service attacks.* Another form of computer attack is the distributed denial of service (DDoS) attack. The DDoS attacker uses multiple compromised systems to attack a single target, thereby causing denial of service for users of the targeted system.[22] The flood of incoming requests to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. DDoS threats have been escalating and future attacks may target routers, key hubs of the Internet's infrastructure, instead of individual web sites.[23]

*Security measures.* There are two primary security measures that companies and individuals use to protect their computer systems from attack: firewalls and anti-virus software. A firewall is a set of related programs located at a network gateway server[24] that protects a private network from users of outside networks.[25] A firewall may also be used to control the outside resources that network users access.[26] Anti-virus software, on the other hand, searches computer systems for any known or potential viruses.

### *The Computer Fraud and Abuse Act*[27]

Computer crimes are primarily addressed by the Computer Fraud and Abuse Act (CFAA).[28] The CFAA makes it unlawful for any person to access a protected computer[29] "without authorization."[30] It also forbids a person who has a legitimate and authorized right of access from "exceeding the authorized access."[31] If either type of access results in the person's obtaining information from the protected computer and the conduct involves interstate or foreign communication, then a violation of the Act is established. The CFAA also prohibits activities such as the dissemination of malicious software[32] and trafficking in stolen passwords.[33] The CFAA allows any person who suffers damage or loss by reason of a violation of the statute to maintain a civil action to obtain compensatory damages and injunctive relief or other equitable relief.[34]

### *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*[35]

On October 26, 2001, the President signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) into law, providing law enforcement with sweeping powers and raising concern among privacy advocates.[36] In essence, the USA PATRIOT Act seeks to protect the National Infrastructure by easing the restrictions placed on electronic surveillance[37] and facilitating the prosecution of cybercrime by amending many provisions in the CFAA. These amendments lower jurisdictional hurdles relating to protected computers and damages, and increase penalties for violations.

*Expanding the scope of "protected computers."* Before the amendments in section 814 of the USA PATRIOT Act, the CFAA defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce or communication."[38] This definition did not explicitly include computers outside the United States. Because of the interdependency of global computer networks, system crackers from within the United States increasingly targeted systems located entirely outside of this country. In addition, computer criminals in foreign countries frequently routed communications through the United States as they gained access from systems located in one foreign country to another. In such cases, the lack of any U.S. victim discouraged U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

Section 814 of the USA PATRIOT Act amends the definition of "protected computer" to clarify that this term includes computers outside of the United States, so long as they affect "interstate or foreign commerce or communication of the United States."[39] This allows the United States to use speedier domestic procedures to join in international computer crime investigations. In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States.

*Defining "loss."* Litigants must prove that an individual caused over $5,000 loss in order to meet the CFAA's jurisdictional requirements found in 1030(a)(5)(B)(i). Prior to section 814's amendments, however, the CFAA had no definition of loss. The only court to address the scope of this term adopted an inclusive reading of what costs litigants may include. In United States v. Middleton,[40] the U.S. Court of Appeals for the Ninth Circuit held that the definition of loss includes a wide range of harms typically suffered by the victims of computer crimes. These harms include costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of interruption of service.[41] Amendments in section 814 codify the broad definition of loss adopted in Middleton.[42]

*Aggregating damages.* Prior to the USA PATRIOT Act's amendments, 18 U.S.C. 1030(e)(8) defined "damage" as:

> any impairment to the integrity or availability of data, a program, a system or information that (A) causes loss aggregating at least $5000 in value during any 1-year period to one or more individuals; (B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more individuals; (C) causes physical injury to any person; (D) threatens public health or safety.

The CFAA was unclear, however, regarding whether prosecutors could aggregate the loss resulting from damage an individual caused to different protected computers in seeking to meet the jurisdictional $5,000 loss threshold. For example, a system cracker could unlawfully access five computers on a network on ten different dates as part of a related course of conduct, but cause only $1,000 loss to each computer during each intrusion. If the CFAA were interpreted not to allow aggregation, then that person would not be liable under the CFAA since he or she had not caused over $5,000 of loss to any particular computer. Under the amendments in section 814 of the USA-PATRIOT Act, one may aggregate "loss resulting from a related course of conduct affecting one or more other protected computers" that occurs within a one year period in proving the $5,000 jurisdictional threshold for damaging a protected computer.[43]

*Clarification of intent to cause damage.* Under previous law, in order to violate subsection (a)(5)(A),[44] an offender had to "intentionally [cause] damage without authorization." Courts, however, have had difficulty in interpreting whether an offender must intend the actual loss suffered by the victim. Section 814 of the USA-PATRIOT Act amended the CFAA to clarify that an individual need only intend to damage the computer or the information on it, and not intend a specific dollar amount of loss or other special harm. The amendments move these jurisdictional requirements to 1030(a)(5)(B), explicitly making them elements of the offense, and define "damage" to mean "any impairment to the integrity or availability of data, a program, a system or information."[45] An actor will violate 1030(a)(5) when he or she causes damage to a protected computer with one of the listed mental states, and the conduct in fact caused either a loss exceeding $5,000, impairment of medical records, harm to a person, or threat to public safety.[46]

*Damaging national security and criminal justice computers.* The CFAA previously had no special provision that would augment punishment for criminals who damage computers used in connection with the judicial system, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over $5,000 loss or meet one of the

CFAA's other special requirements. These systems, however, serve critical functions and arguably justify felony prosecutions even where the damage is relatively slight. Amendments in section 814 of the USA PATRIOT Act create section 1030(a)(5)(B)(v) to address this issue. Under this provision, a criminal violates federal law by damaging a computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," even if that damage does not result in provable loss over $5,000.

*Raising penalties and eliminating mandatory minimums.* Under previous law, first-time offenders who violate section 1030(a)(5)[47] could be punished by no more than five years' imprisonment, while repeat offenders could receive up to ten years. It was argued, however, that this five-year maximum did not adequately take into account the seriousness of their crimes.[48] In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4).[49] Section 814 of the USA PATRIOT Act raises the maximum penalty for violations arising out of damage to protected computers to ten years for first offenders, and twenty years for repeat offenders.[50] Congress also chose to eliminate all mandatory minimum guidelines sentencing for section 1030 violations. New legislation has also been introduced to further increase these penalties.[51]

## Government Search & Seizure[52]

The government must monitor cyberspace in order to detect and prevent attacks on the National Infrastructure. Privacy enhancing technology, such as encryption and anonymous networks, challenge such surveillance. Government agents who employ counter-methods to circumvent these technologies, however, are subject to statutory and procedural constraints. These limitations are designed to protect civil liberties such as privacy and freedom of speech, and failure to follow the established rules can lead to criminal and civil liability.

### *Privacy Enhancing Technology*

Privacy Enhancing Technology (PET) are important tools that facilitate civil liberties such as privacy and freedom of speech by protecting individuals from government surveillance and censorship.[53] This technology may also be used, however, to conceal the identity and communications of computer criminals who seek to damage the National Infrastructure. This technology, therefore, creates obstacles to efficient law enforcement.[54]

*Encryption*. Encryption (also called "cryptography") is used to secure information by converting data into "ciphertext" so that it is not easily understood by unauthorized people.[55] Encryption generally contains two components:

1. Cryptography: the improvement of methods for keeping data secure from unauthorized parties, and
2. Cyptanalysis: the circumvention of cryptographic codes.

There are many products available for users to utilize encryption technology.[56] In the context of the National Infrastructure, network encryption (sometimes called "network layer," or "network level" encryption) is used to secure communications within a network by applying cryptography at the network transfer layer.[57]

Governments have traditionally attempted to improve national security and facilitate domestic law enforcement by weakening cryptography. This usually occurs by either imposing export controls that inhibit the spread of cryptographic innovations[58] or by requiring "backdoors," called "government escrow,"[59] that provide law enforcement agents the ability to decode the encryption scheme. It has been argued that when a government acts to weaken cryptography, it concomitantly strengthens criminal cryptanalysis and destabilizes intellectual and financial property.[60]

*Anonymizing technology.* There is a wide spectrum of competency and motives amongst people who want their online identity to remain hidden.[61] Anonymous networks provide one of the most comprehensive forms of anonymity in electronic communications. Anonymous networks exists as a "parallel" Internet, where content of any kind can be uploaded and downloaded without any way to track who created a given site or to take down a given piece of content once it is in the network. These anonymous networks are comprised of volunteers who give up portions of their hard drives as nodes, or storage centers, within the network. Chief among these providers is Freenet,[62] an open-source project viewed by many as the successor to Napster's original promise of free online file swapping.[63]

### *Surveillance Technology*

Preventing and prosecuting cybercrime requires government agents to ascertain the identity of criminals in cyberspace. This is typically accomplished by tracing the Internet Protocol (IP) address of each node along the path of the user's electronic communication.[64] This electronic trail has been called the "fingerprint of the twenty-first century," only it is much harder to find and not as permanent as its more traditional predecessor.[65] Surveillance technology makes such identification possible by searching networks for specific types of data, providing "back doors" into suspect's systems and wide-scale monitoring of communications.

*Carnivore (DCS1000).* Carnivore is, in essence, a special filtering tool that gathers information authorized by court order.[66] Carnivore monitors large volumes of traffic passing through ISP facilities and reportedly captures only those data packets that law enforcement has legal authorization to collect.[67] Carnivore is reportedly subject to several technical deficiencies.[68] For instance, problems may arise while attempting to track dynamically assigned IP addresses.[69] Also, "[t]here is a question of whether Carnivore could distinguish real network traffic versus traffic generated to trick the technology."[70]

*Keyboard Logging Systems.* Keyboard Logging Systems (KLS) use remotely installed software to capture the keystrokes of suspected criminals and transmits this information to agents in real time.[71] By tracking exactly what a suspect types, encryption key information can be gathered and transmitted back to law enforcement.[72] For example, under a project named "Magic Lantern," the Federal Bureau of Investigations (FBI) allegedly created a Trojan horse to facilitate KLS infiltration of suspects computer systems.[73] The FBI, naturally, has been reluctant to release information regarding Magic Lantern for review.

*ECHELON*. ECHELON is an automated global interception and relay system reportedly operated by intelligence agencies in five nations: the United States, the United Kingdom, Canada, Australia, and New Zealand.[74] According to reports, it is capable of intercepting and processing many types of transmissions, throughout the globe. It has been suggested that ECHELON may intercept as many as three billion communications every day, including phone calls, e-mail messages, Internet downloads, satellite transmissions, etc. There has been a global response to the ECHELON system resulting in counter-technological systems[75] and code designed to attract the attention of the ECHELON system.[76] Many countries have also expressed concern regarding the parameters participants in the ECHELON system will follow in deciding whether to disclose information gathered by the system to third parties.[77]

### *Statutory Framework*

The law governing surveillance of electronic communications has two primary sources: the Fourth Amendment to the U.S. Constitution and the statutory privacy laws codified at 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-11, 18 U.S.C. §§ 3121-27 and 47 U.S.C. §§ 1001 et seq. Although constitutional and statutory issues overlap in some cases, most surveillance present either a constitutional issue under the Fourth Amendment or a statutory issue under these four statutes.

*Fourth Amendment.*[78] The Fourth Amendment was originally adopted to address the tension between privacy and public safety. Its goal is to preserve privacy while protecting the safety of U.S. citizens. A search will satisfy the Fourth Amendment if it does not violate a person's "reasonable" or "legitimate" expectation of privacy.[79] This inquiry embraces two discrete questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[80] No bright line rule indicates whether an expectation of privacy is constitutionally reasonable.[81] If a search will violate an individual's reasonable expectation of privacy, the government must obtain a warrant prior to conducting the search by demonstrating probable cause. The modern legal framework for computer privacy and electronic surveillance arises out of the Supreme Court's landmark decision in Katz v. United States.[82] Prior to Katz, the Supreme Court had regarded wiretapping as outside the scope of the Fourth Amendment's restrictions on unreasonable searches and seizures.[83] In Katz, the Supreme Court reversed its prior position and held for the first time that Fourth Amendment protections apply to government interception of telephone conversations. By 1968, however, the provisions of the Act dealing with wiretapping had become so muddled by inconsistent interpretations of federal and state courts that Congress intervened and drafted what would come to be known as the Wiretap Act.[84]

*Wiretap Act.[85]* The Wiretap Act, commonly known as "Title III," prohibits the intentional interception of any "wire, oral or electronic communication."[86] This Act created the foundation for communication privacy and electronic surveillance law by establishing a judicial process by which law enforcement officials may obtain lawful authorization to conduct electronic surveillance and prohibiting the use of electronic surveillance by private individuals. A subsequent amendment to Title III also requires telecommunications carriers to "furnish [law enforcement] . . . all information, facilities, and technical assistance necessary to accomplish [an] interception."[87]

*Electronic Communications Privacy Act of 1986.[88]* In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"), which extended the prohibitions contained in Title III to electronic communications that are intercepted contemporaneously with transmission.[89] Among the ECPA amendments to Title III were requirements that:

1. Interceptions be conducted unobtrusively and with a minimum of interference with the services of the person whose communications are being intercepted; and
2. The interception is conducted in such a way as to minimize access to communications not otherwise authorized for interception.[90]

The ECPA classifies electronic communications according to privacy interests that are implicated by the information sought. [91] For example, disclosure of stored e-mails involves a different privacy interest than providing subscriber account information. The ECPA also subjects computing services available "to the public" to more strict regulation than services that are not available to the public. To protect these privacy interests, ECPA offers varying degrees of legal protection depending on the perceived seriousness of the privacy interest involved.[92] With certain exceptions, the ECPA criminalizes and creates civil liability for intentionally intercepting electronic communications without a judicial warrant.[93] Under the ECPA, good faith reliance on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization is a defense to causes of action based on the disclosure of such information.[94]

*Stored Communications Act.[95]* The Stored Communications Act, Title II of the ECPA, provides protection for messages while they are in the course of transmission.[96] The Act applies to messages that are stored in intermediate storage temporarily, after the message is sent, but before it is retrieved by the intended recipient.[97] It is a violation of the Stored Communications Act to "access without authorization a facility through which an electronic information service is provided ... and thereby obtain ... access to a wire or electronic communication while it is in electronic storage in such system . . . ."[98] The Stored Communications Act, therefore, does not apply to messages acquired after transmission to the intended recipient is complete.

*Communications Assistance for Law Enforcement Act (CALEA).[99]* Since 1970, telecommunications carriers have been required to cooperate with law enforcement personnel in conducting lawfully authorized electronic surveillance.[100]

The Communications Assistance for Law Enforcement Act (CALEA) expanded these requirements by mandating telecommunications carriers to modify the design of their equipment, facilities, and services to ensure that lawfully authorized electronic surveillance can actually be performed.[101] CALEA also imposes certain responsibilities on the Attorney General of the United States,[102] the Federal Communications Commission (FCC),[103] telecommunications equipment manufacturers,[104] and telecommunications support services providers.[105] On February 24, 1995, the Attorney General delegated management and administrative responsibilities for CALEA to the FBI.[106] The FBI, in turn, created the CALEA Implementation Section (CIS), which works with the telecommunications industry and the law enforcement community to facilitate effective and industry-wide implementation of CALEA.[107]

*Pen Register and Trap-and-Trace Statute.*[108] The Pen Register and Trap-and-Trace Statute ("Pen/Trap Statute") permits the government to install devices that record and decode electronic signals used in call processing.[109] Essentially, this equipment is used to determine the source and destination of wire and electronic communications. When Congress enacted the Pen/Trap Statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks.[110]

Although numerous courts across the country have applied the Pen/Trap Statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. Moreover, certain private litigants have challenged the application of the Pen/Trap Statute to such electronic communications based on the statute's telephone-specific language. Section 216 of the USA-PATRIOT Act[111] addressed these issues by amending the Pen/Trap Statute in three important ways:

1. The amendments clarified that law enforcement may use Pen/Trap orders to trace communications on the Internet and other computer networks[112];
2. Pen/trap orders issued by federal courts have nationwide effect[113]; and
3. Law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider.[114]

### *Intercepting Communications*

Procedural safeguards limit the government's ability to monitor electronic communications. These limitations require government agents to procure court approval prior to monitoring and gathering electronic evidence. Generally, government agents will need a subpoena to obtain information identifying a subscriber,[115] a court order to obtain transactional records identifying the source and destination of communications,[116] a warrant to obtain the actual content of electronic communications,[117] and a wiretap order to intercept communications as they occur.

Because of the privacy values it protects, Title III and the ECPA places the highest burden on the real-time interception of oral, wire, and electronic communications.[118] As such, in the absence of a statutory exception, the government needs a court order to wiretap electronic communications. To obtain such a wiretap order (also called a "Title III order"), the government must show that normal investigative techniques for obtaining the information have or are likely to fail or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.[119] The remedies for violating Title III or the ECPA by improperly intercepting electronic communications without a warrant can include criminal sanctions, civil suit, and for law enforcement agents, adverse employment action.[120] Objectively reasonable good faith reliance on a warrant, court order, or statutory authorization is a complete defense to such violations.[121]

It is important to note that the government will not always need to seek a court's approval when conducting surveillance. For example, if the government's conduct does not violate a person's "reasonable expectation of privacy," then formally it does not constitute a Fourth Amendment "search" and no warrant is required.[122] Also, a warrantless search that violates a person's reasonable expectation of privacy will nonetheless be "reasonable" and, therefore, constitutional if it falls within an established exception to Title III's requirements.[123] Three common exceptions exist.[124] Generally, procedural hurdles can be overcome when victims consent to government monitoring of their own conversation, when victims independently monitor their own conversation after they have suffered damage or when service providers pro-actively monitor services to protect their network.

*Consent of a party "acting under color of law."* The most widely used exception to Title III permits "a person acting under color of law" to intercept an electronic communication where "such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception."[125] In the context of electronic communications, two circuits have recognized that a computer owner may be considered a "party to the communication" and thus can consent to the government monitoring electronic communications between that computer and a network trespasser.[126] Under this exception, therefore, it has been held that a victim may monitor, and authorize the government to monitor, system intrusions directly with his or her computer.[127]

*Consent of a party "not acting under color of law."* Title III also permits "a person not acting under color of law" to intercept an electronic communication where "such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception."[128] This exception permits a victim to monitor communications to which he or she is a party before law enforcement gets involved. Also, it allows law enforcement to obtain the implied consent of the subject intruder through computer "banners," which alert network participants that monitoring is taking place prior to entering the network.[129] A properly worded banner results in the trespasser's implied consent to monitoring of all downstream activities, thus alleviating Title III concerns.

*Protecting providers' rights and property.* Title III also permits electronic communication providers to intercept communications as a "necessary incident to the rendition of his service" or to protect "the rights or property of the provider of that service."[130] This exception allows private parties to monitor their system to prevent misuse. Since network intrusion often involves damage or disabling of a network's computer security system, as well as theft of the network's service, this exception permits a system administrator to monitor the activities of a system cracker while on the network.

This exception to Title III has some significant limitations. One important limitation is that the monitoring must be reasonably connected to the protection of the provider's service and not as a pretext to engage in unrelated monitoring. This is due to the fact that the right to monitor is justified by the right to protect one's own system from harm. An ISP, therefore, may not be able to monitor the activities of one of its customers under this exception for allegedly engaging in unlawful activities on other networks. This limitation also makes it difficult for a network administrator to justify monitoring activities when the subject jumps to a new downstream victim.[131]

## Private Search & Seizure

Private parties are subject to fewer restrictions than government agents are when monitoring attacks on the National Infrastructure. American policymakers and strategists must recognize the value of such individuals and foster the hacking community's willingness to aid the government in protecting critical systems. In order to maximize the effectiveness of their contributions and avoid statutory liability, hacktivists must know what kinds of information is most valuable, how they can coordinate with government actors without becoming an agent of the government, and what privacy protections users possess when traveling through networks.

### *Fourth Amendment*

As a general matter, the Fourth Amendment does not apply to searches conducted by private parties who are not acting as agents of the government. Courts have held that the Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official."[132] As a result, no violation of the Fourth Amendment occurs when a private individual acting on his own accord conducts a search and makes the results available to law enforcement.[133] Of course, statutory protections also exist that generally protect the privacy of electronic communications stored remotely with service providers, and can protect the privacy of Internet users when the Fourth Amendment may not.[134]

In United States v. Hall,[135] the defendant took his computer to a private computer specialist for repairs. In the course of evaluating the defendant's computer, the repairman observed that many files stored on the computer had filenames characteristic of child pornography. The repairman accessed the files, saw that they did in fact contain child pornography, and then contacted the state police. The tip led to a warrant, the defendant's arrest, and his conviction for child pornography offenses. On appeal, the U.S. Court of Appeals for the Seventh Circuit rejected the defendant's claim that the repairman's warrantless search through the computer violated the Fourth Amendment. Because the repairman's search was conducted on his own, the court held, the Fourth Amendment did not apply to the search or his later description of the evidence to the state police.[136]

### *When Private Parties Become Government Agents*

The fact that the person conducting a search is not a government employee does not necessarily mean that a search is "private" for Fourth Amendment purposes. A search by a private party will be considered a Fourth Amendment government search "if the private party act[s] as an instrument or agent of the Government."[137] Unfortunately, the Supreme Court has offered little guidance regarding when private conduct can be attributed to the government. Instead, the Court has merely stated that this question "necessarily turns on the degree of the Government's participation in the private party's activities . . . a question that can only be resolved 'in light of all the circumstances.'"[138]

In the absence of a more definitive standard, the various federal courts of appeals have adopted a range of approaches for distinguishing between private and government searches. About half of the circuits apply a "totality of the circumstances" approach that examines three factors:

1. Whether the government knows of or acquiesces in the intrusive conduct;
2. Whether the party performing the search intends to assist law enforcement efforts at the time of the search; and
3. Whether the government affirmatively encourages, initiates, or instigates the private action.[139]

Other circuits have adopted more rule-like formulations that focus on only certain aspects of these factors.[140]

### *Voluntary Disclosure*

Government agents occasionally seek the permission of a network's "system administrator" or "system operator" to search the content of an account holder.[141] As a practical matter, the primary barrier to searching a network account pursuant to a system administrator's consent is statutory, not constitutional.[142] System administrators usually serve as agents of "provider[s] of electronic communication service" under the ECPA and the ECPA regulates law enforcement efforts to obtain the consent of a system administrator to search an individual's account.[143] Accordingly, any attempt to obtain a system administrator's consent to search an account must comply with ECPA. To the extent that ECPA authorizes system administrators to consent to searches, the resulting searches will in most cases comply with the Fourth Amendment. This is due to the fact that individuals may not retain a reasonable expectation of privacy in the remotely stored files and records that their network accounts contain.

Section 212 of the USA-PATRIOT Act[144] amended subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person.[145] This voluntary disclosure does not, however, create an affirmative obligation to review customer communications in search of such imminent dangers. The amendments in section 212 also change the ECPA to allow providers to disclose information to protect their rights and property by enacting two related sets of amendments.[146] First, amendments to sections 2702 and 2703 of Title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to section 2702. Thus, section 2702 now regulates all permissive disclosures of content and non-content records alike, while section 2703 covers only compulsory disclosures by providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers have the statutory authority to disclose non-content records to protect their rights and property.

### *Limits to Government Use*

The fact that a private person has uncovered evidence of a crime on another person's computer does not permit agents to search the entire computer. Instead, the private search permits the agents to view the evidence that the private search revealed, and, if necessary, to use that evidence as a basis for procuring a warrant to search the rest of the computer. In United States v. Jacobsen,[147] the Supreme Court presented the framework that currently guides government agents who seek to uncover evidence as a result of a private search. Under Jacobsen, agents who learn of evidence via a private search can reenact the original private search without violating any reasonable expectation of privacy. What the agents cannot do without a warrant is "exceed[] the scope of the private search."[148] This standard requires agents to limit their investigation to the precise scope of the private search when searching without a warrant after a private search has occurred. So long as the agents limit themselves to the scope of the private search, the agents' search will not violate the Fourth Amendment. However, as soon as agents exceed the scope of the private warrantless search, any evidence uncovered may be suppressed.[149]

## Looking Forward

"It takes networks to fight networks."[150] Governments that seek to counter networked crime and terrorism will need to adopt organizational designs and strategies that emulate those of their adversaries. Although these principles depend upon technological innovation, they are more contingent on a willingness to innovate organizationally and doctrinally. If government agencies become ready and willing to rely on networks of "ethical hackers" in times of crisis, the need to coordinate beyond the boundaries of government will increase.

### *Government Actions*

The frequency of computer attacks has exponentially increased in recent years, requiring the government to take more seriously the threats posed by cybercrime and netwar to our nation's National Infrastructure.[151] Recent measures include:

- Allocating funds to increase the resilience of the National Infrastructure[152];
- Introducing legislation to limit government disclosure of successful attacks[153];
- "Encouraging" private parties to share information relating to successful attacks[154];
- Removing certain information from government web sites[155];
- Forming governmental-corporate alliances[156];
- Disabling suspected terrorist-supported web sites[157];
- Updating government encryption standards[158]; and
- Proposing government-only networks[159] and cybercrime-specific courts.[160]

Taking the lead in securing the National Infrastructure are the Bush Administration's Special Advisor for Cyberspace Security,[161] Critical Infrastructure Protection Board (CIPB)[162] and National Infrastructure Advisory Counsel (NIAC),[163] the newly reorganized Federal Bureau of Investigations (FBI),[164] and the Office of Homeland Security (OHS).[165]

### *Government Alliances*

Private industry and "white hat" hackers [166] have begun to offer up their services to the government through various initiatives. For instance, the Cult of the Dead Cow (cDc)[167] and Microsoft[168] have both reportedly offered assistance to the FBI's Magic Lantern initiative, which was used to develop the FBI's keyboard logging software.[169] Individuals have also taken it upon themselves to assist law enforcement's prosecution of child pornography through various technological means. Individuals have reportedly developed a viral code that infiltrates recipients' computers, searches for file names that could contain child pornography, and reports results to law enforcement agencies.[170]

Concern has been raised regarding the degree of cooperation and coordination these groups have provided to aid the government prosecution of cybercrime and protection of the National Infrastructure. Much like escrow encryption,[171] privacy groups and software manufacturers are especially anxious that cooperation between software providers and government agencies could lead to agreements wherein providers would purposefully avoid updating anti-virus tools to detect such a Trojan.[172] It is, of course, generally accepted by the security community that it would be irresponsible to build a safety critical computer system that would be vulnerable to such interventions.

### *Independent Initiatives*

Hacktivists can aid in the defense of the National Infrastructure by testing critical systems, identifying potential weaknesses, monitoring suspicious activity in cyberspace and, possibly, aiding in retaliatory attacks on hostile governments. For instance, private groups have already taken it upon themselves to retaliate for attacks to the U.S. National Infrastructure. In April 2001, for example, Chinese hackers were reportedly encouraged to hack U.S. sites as tensions between the United States and China escalated in response to the downing of a U.S. fighter jet.[173] Nine government and commercial Web sites, including two Navy sites, were reportedly vandalized since the standoff began on April 1, 2001. American hacker group PoizonBOx allegedly responded by defacing at least a hundred Chinese Web sites since April 4, 2001.[174] Another hacktivist group, Hacktivismo,[175] responded to China's alleged censorship initiatives entitled "the Great Firewall of China" and "the Golden Shield"[176] through the creation of software called "Peekabooty." Much like anonymous networks,[177] Peekabooty allegedly enables individuals living in oppressive regimes to access prohibited material through fellow Peekabooty clients located in more liberal countries.[178]

### *Policy Considerations*

Without the ability to protect itself, a democratic society cannot exist. In order to remain a democratic nation, however, our security must be guided by the time-tested constitutional principle of privacy. If law enforcement fails to properly respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. In America, we define the right to privacy according to what our society is prepared to recognize as reasonable.[179] The issue therefore becomes: "What protective measures does our society deem to be reasonable when ensuring the security of our National Infrastructure?"

Recent legislative reforms attempt to secure the National Infrastructure by increasing governmental surveillance power and easing the prosecution of computer-related crimes. These measures were rapidly implemented in response to terrorist attacks and did not result from the extensive, focused debate that typically characterizes such sweeping legislation. Many feel that Congress, acting in midst of a crisis, did not pay ample attention to what "protection" means in a today's networked society. Policy makers may have lacked sufficient information to address from what (and from whom) America should seek to protect its National Infrastructure. Moreover, critics question whether such conventional tactics will be effective when confronted with the novel threat of netwar. In fact, such actions may actually hinder the National Infrastructure by discouraging beneficial hacktivism for fear of prosecution, and instilling enmity between hacktivists and law enforcement, while concomitantly restraining civil liberties. Far better would be to foster a sense of civic duty among groups of ethical hackers, revise existing laws to facilitate cooperation between hacktivists and law enforcement, and develop innovative programs that encourage responsible hacktivism[180] and fuel hacktivists' innate love of a good challenge.[181]

## Conclusion

For better or for worse, our society is dependent on computer networks to support its National Infrastructure. We must create a framework for understanding the relationship between technology, law, and policy in this networked world to ensure that democracy remains viable as we move into the twenty-first century. Our security will require vigilance and education in the hacking community, understanding and innovation among government actors, and acknowledgement of the useful role that each party plays. In a very real way, we are each a "node" in this network, contributing to the vulnerability and safety of our nation. We must work together to identify our weaknesses, propose viable solutions, and rise to meet the challenges that face our increasingly connected society.

## Notes

1. For a description of the various components that make up the National Infrastructure, see the National Infrastructure Protection Center FAQ, at <www.nipc.gov/about/about5a.htm>.
2. Word Net, Princeton University, available at <www.dictionary.com/search?q=network>.
3. See William J. Holstein, Lessons from Networks, Online and Other, *N.Y. Times* (June 23, 2002), available at <www.nytimes.com/2002/06/23/business/yourmoney/23VALU.html>.
4. See generally Yochai Benkler & Alan Toner, Access to the Internet (June 12, 2001), available at <eon.law.harvard.edu/ilaw/Access/>.
5. For graphical representations of these networks, see John Arquilla and David Ronfeldt, The Advent of Netwar (Revisited), Rand p. 8, available at <www.rand.org/publications/MR/MR1382 MR1382.ch1.pdf> (Netwar Revisited).
6. It has been stated that the amount of data storage that a microchip can hold doubles approximately every eighteen months. This is called Moore's Law, attributed to Gordon Moore, co-founder of Intel Corporation. A definition of Moore's Law with referenced articles is available at <whatis.techtarget.com/definition/0,,sid9_gci212591,00.html>.
7. The value of a network is a function of the number of users connected to the network and the number of interconnections between users. This is called Metcalfe's Law, attributed to Robert Metcalfe, a pioneer of computer networking. A definition of Metcalfe's Law with referenced articles is available at <searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214115,00.html>.
8. See Commission on National Security/21st Century Report, available at <www.nssg.gov./Reports /reports.htm>. Also see Barton Gellman, U.S. Finds Clues to Potential Cyber-attack, The Mercury News (June 27, 2002), available at <www.siliconvalley.com/mld/siliconvalley/3554402.htm> (discussing the National Infrastructure Protection Center's concern that physical attacks to the United States could be made in conjunction with attacks on the our nation's 911 system and power grid).
9. See U.S. House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations House Report (stating that two-thirds of federal agencies, including the departments of Defense, Commerce, Energy, Justice, and Treasury received "F" grades). Also see House Subcommittee On Oversight And Investigations Hearing, Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems? (April 2001) (citing a series of General Accounting Office reports to criticize the state of computer security throughout the federal government since 1996).
10. Netwar Revisited at 6.
11. A definition of "hacktivism" is available at <searchsecurity.techtarget.com/sDefinition /0,,sid14_gci552919,00.html>.
12. Although this paper uses the term "hacker" to describe individuals who gain unauthorized access to computer systems, this is not the terminology such individuals use to describe themselves. "Hacker" is a generic term used by computer programmers to mean "a clever programmer." Computer programmers take issue with the use of the term "hacker" to describe individuals who gain unauthorized computer access. Instead, the term "cracker" is used to describe people who intentionally breach computer security systems. A system cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or simply because the challenge is there.
13. Generally, hacktivists typically target sites that are run by governmental, educational, commercial, and cultural institutions. Often, the hacktivist will merely leave a message on the home page of the

target site or launch a denial-of-service attack to disrupt traffic to a particular site. See Section II.A infra, entitled "Technology and Targets," for an overview of these tools and methods.

14. In discussing cybercrime, a distinction must be made between technological acts that constitute a crime (i.e., a violation of established law) and those acts that merely constitute a violation of a private agreement and/or industry standard (i.e., a violation of a website's terms of service). What is commonly referred to as "computer fraud" or "cybercrime" involves a criminal act, while mere "computer abuse" deals with violations of an organization's computer use policies and lacks a criminal act. See Cybercrime Documents: Press releases, speeches, Congressional testimony, letters, reports, manuals, and court filings related to computers and cyberspace, available at <www.usdoj.gov/criminal/cybercrime/docs.html#docg>.
15. As such, many blame large computer manufacturers such as Microsoft for failing to develop comprehensive policies and procedures for dealing with increasingly sophisticated attacks and failing to implement security regimes in their products. Increasing frustration with technology providers has lead policy makers such as Rep. Rick Boucher (D-Va.) to call for liability for product defects that result in security breaches. Section 814 of the USA PATRIOT Act, however, modified the civil damages subsection of 18 U.S.C. 1030(g) to include a provision which states that "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."
16. In programming, a "port" is a "logical connection place" where a client program specifies a particular server program on a computer in a network.
17. Although the most secure passwords include random or partly random series of numbers, symbols, and letters, many use passwords that are easy to remember and often write them down for quick reference or use the same passwords for multiple functions. Even carefully chosen passwords, however, are vulnerable to sophisticated password-cracking programs. Some password crackers use "word lists": lists of words, phrases, or other combinations or letters, numbers and symbols that computer users often use as passwords. Others use "brute-forcing" techniques, which use every combination and permutation of characters, even nonsensical combinations.
18. A virus is a program that copies itself into other programs and becomes active when a program is run (e.g., clicked on); from there, a virus infects other files. A definition is available at <searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213306,00.html>.
19. A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. A Trojan horse may be widely redistributed as part of a computer virus. A definition is available at <searchsecurity.techtarget.com /sDefinition/0,,sid14_gci213221,00.html>. See Section V.B infra, entitled "Government Alliances," for a description of how the government has used private parties to install Trojans on suspects' computers.
20. A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. A definition of "worm" is available at <searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213386,00.html>.
21. McAfee has posted a map of the world on its site, showing the prevalence of viruses around the world, available at <mast.mcafee.com>.
22. For a description of various DDoS attacks, see <searchsecurity.techtarget.com/sDefinition 0,,sid14_gci557336,00.html>.
23. The most potentially devastating attacks would be directed at Network Access Points (NAPs) and Domain Name Servers (DNS). The primary Internet nodes, also called "top-tier" connection points, are comprised of NAPs that tie all Internet access providers together. The DNS is the Internet's global addressing system responsible for resolving domain name requests to the appropriate Internet Protocol address. Simultaneously targeting such points could cause a cascading effect, bringing all Internet communications to a halt. See Trends in Denial of Service Attack Activity (Oct. 2001), available at <www.cert.org/archive/pdf/DoS_trends.pdf>.
24. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.
25. Basically, a firewall works closely with a router program to examine each network packet and

determine whether to forward it toward its destination. A firewall also works with a proxy server that makes network requests on behalf of workstation users.

26. There are several firewall screening methods. Sometime requests are screened to make sure they come from acceptable (i.e., previously identified) domain name and Internet Protocol addresses.
27. 18 U.S.C. 1030, available at <www4.law.cornell.edu/uscode/18/1030.html>.
28. 18 U.S.C. 1030, available at <www4.law.cornell.edu/uscode/18/1030.html>.
29. As used in the CFAA, a "protected computer" includes any computer "which is used in interstate or foreign commerce or communication." This gives Congress the ability to exercise federal power over all computers involved in interstate and foreign commerce, whether or not any federal government proprietary interest is implicated. See Section II.C infra, entitled "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," for the USA PATRIOT Act's amendments to this definition.
30. 18 U.S.C. 1030(a).
31. Id. The CFAA carefully limits the meaning of "exceeding authorized access" to encompass only the obtaining or altering of information that the person accessing the data is not entitled to obtain or alter.
32. 18 U.S.C. 1030(a)(5)(A).
33. 18 U.S.C. 1030(a)(6).
34. 18 U.S.C. 1030(g).
35. Pub.L. 107-56, Oct. 26, 2001, 115 Stat. 272 (codified in 8 U.S.C. §§ 1226a, 1379; 15 U.S.C. § 1681v; 18 U.S.C. §§ 175b, 1993, 2339, 2712; 22 U.S.C. §§ 262p-4r, 7210, 7211; 31 U.S.C. §§ 310, 311, 5318A, 5319; 42 U.S.C. §§ 3714, 3796c-1, 5195c; 49 U.S.C. § 5103a; and 50 U.S.C. §§ 403-5b to 403-5d, 1861, 1862), available at <216.110.42.179/docs/usa.act.final.102401.html>.
36. See, e.g., EFF Analysis Of The Provisions Of The USA PATRIOT Act (Oct. 31, 2001), available at <www.eff.org/Privacy/Surveillance/Terrorism_militias20011031_eff_usa_patriot_analysis.html>. One particularly controversial aspect of the anti-terrorism law expands a secret court created in 1978 by the Foreign Intelligence Surveillance Act and permits the court's search warrants and eavesdropping orders to apply in domestic investigations.
37. See Section III.C infra, entitled "Statutory Framework," for a discussion of the USA PATRIOT Act's application to surveillance, as opposed to the prosecution of cybercrime. Legislative history of the USA PATRIOT Act is available at <www.cdt.org/security/010911response.shtml>.
38. 18 U.S.C. 1030(e)(2). The first incarnation of the CFAA was passed in 1984 to protect classified information maintained on federal government computers and to protect financial records and credit information stored on financial institution computers. Congress has broadened the scope of the CFAA several times, once in 1986 when certain amendments extended protection to "federal interest computers" and again in 1996, when the phrase "protected computer" replaced the previous concept of "federal interest computer." The latter amendments extended the federal law of computer crime, and the jurisdiction of the federal courts, to protect any computer that is connected to the Internet against certain forms of wrongful computer use.
39. 18 U.S.C. 1030(e)(2)(B). Also see infra note 41, discussing the U.S. v. Ivanov case. It is possible that while the amendment extends the CFAA only to computers located outside the United States, the Ivanov case also extends the statute's ambit to individuals residing outside the United States.
40. 231 F.3d 1207, 1210-11 (9th Cir. 2000).
41. A related question under the CFAA is establishing whether the suspect obtained "anything of value" which is a separate question from damages. In U.S. v. Czubinski, for instance, the First Circuit found that browsing confidential taxpayer information was not the same as obtaining "anything of value" because the value of something is "relative to one's needs and objectives." 106 F3d 1069, 1078. Cf. U.S. v. Ivanov, where the defendant obtained "root access" to a system and then tried to extort money from the machine's owner. The court there held that gaining root access gave the defendant control over the machine and thus he had obtained "value" for purposes of 1030(a)(4). 175 F.Supp.2d 367, 371-2 (D.Conn. 2001).
42. 18 U.S.C. 1030(e)(11).
43. 18 U.S.C. 1030(a)(5)(B)(i).
44. 18 U.S.C. 1030(a)(5)(A) provides liability for "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."
45. 18 U.S.C. 1030(e)(8).

46. See 18 U.S.C. 1030(a)(5)(B).
47. This section addresses situations where an individual "(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage."
48. For example, David Smith pled guilty to violating section 1030(a)(5) for releasing the "Melissa" virus that damaged thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over $80,000,000 worth of loss (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real loss was as much as ten times that amount.
49. This section addresses situations where an individual "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."
50. 18 U.S.C. 1030(c)(4).
51. The Cyber Security Enhancement Act (CSEA) would increase penalties for computer intrusions, funds surveillance research, and encourages Internet providers to turn over more information to police. The CSEA is sponsored by Crime Subcommittee chairman Lamar Smith (R-Texas). See Declan McCullagh, Cybercrime Bill Ups the Ante (Feb. 12, 2002), available at <www.wired.com/news/politics/0,1283,50363,00.html>.
52. For a comprehensive analysis of search and seizure in the context of computers see Computer Crime Section DOJ: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, available at <www.cybercrime.gov/searchmanual.htm> ("DOJ Search Manual").
53. Other methods of maintaining anonymity include creating forged e-mail headers with readily available software tools, jumping from compromised network to compromised network, using "free-trial" accounts, or by "wiping clean" logging records that would be evidence of their activity.
54. To complicate matters further, victims may be unaware of criminal activity on their network or, if aware, slow or unwilling to report it due to competitive reasons. Many victims and ISPs also fail to record, or preserve for a sufficient length of time, historical logs and other records that might otherwise lead to the identification of attackers.
55. There is relatively little benefit from cryptography, however, unless the user has first secured his LAN and/or stand-alone PC. See Section III.B.2 infra, entitled "Keyboard Logging Systems," for a description of one method to circumvent encryption.
56. Such products include Pretty Good Privacy (PGP) and Public Key Infrastructure (PKI), which allows users to ensure that financial information, health records, and other information that will only go to those who are entitled to view the information.
57. This is a layer in the OSI (Open Systems Interconnection). A description of OSI is available at <searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212725,00.html>.
58. Strong crypto is generally exportable, but in many cases companies are still required to submit a copy of new software to the U.S. government for a thirty-day review. Open source code has fewer restrictions, except when part of a commercial product.
59. Government escrow enables the government to access encrypted private communication. See, e.g., Electronic Privacy Information Center, The Clipper Chip, available at http://www.epic.org/crypto/clipper.
60. See Eben Moglen, So Much For Savages, Comments on Encryption Policy, NYU Law School, November 19, 1998 (revised) (arguing that government escrow of security software will lead to greater threats from computer criminals. Firstly, backdoor encryption will require a backdoor in the global financial system, which is dependant on secure encryption. These backdoors may weaken the global financial system's security and raise the possibility of attacks by ordinary as well as politically motivated criminals against the global financial structure.), available at <old.law.columbia.edu/my_pubs/yu-encrypt.html>.
61. When analyzing the benefit of such technology, the reader should keep in mind that the anonymizing

technology that help criminals avoid identification can also be used to aid undercover law enforcement agents.

62. <www.freenetproject.org/>.
63. Other providers include Cryptobox (<sourceforge.net/projects/cryptobox/>) and Safeweb (<www.safeweb.com/>). But see David Martin and Andrew Schulman, Deanonymizing Users of the Safeweb Anonymizing Service (Feb. 12, 2002) (discussing flaws in SafeWeb's architecture, which potentially allow adversaries to turn SafeWeb into a weapon against its users), available at <www.cs.bu.edu/techreports/pdf/2002-003-deanonymizing-safeweb.pdf>.
64. An alternative to this method, typically used as a last resort, is to examine the communication for "fingerprints" of the poster. These are telltale habits or tendencies that can be compared with other, less anonymous posts. Unusual capitalization, favorite slang terms or phrases, and unique sentence patterns can be used to narrow down the field.
65. See Statement of Kevin V. DiGregory Deputy Assistant Attorney General United States Department of Justice Before the Subcommittee on the Constitution of the House Committee on the Judiciary on The Fourth Amendment and the Internet (Apr. 6, 2000), available at <www.cybercrime.gov/inter4th.htm>.
66. See Section 3.E infra, entitled "Intercepting Communications," for a description of court orders.
67. See FBI Press Release , available at <www.fbi.gov/programs/carnivore/carnivore.htm>.
68. Illinois Institute of Technology Research Institute, Commissioned by the U.S. Justice Department, found several shortcomings in Carnivore. The Justice Department is expected to present the results of an internal review of Carnivore, along with recommended changes, to Attorney General John Ashcroft.
69. James Evans, Concerns Remain About FBI's 'Carnivore' Wiretap, CNN.Com (Mar. 12, 2001), available at <www.cnn.com/2001/TECH/internet/03/12/carnivore.concerns.idg>. Many corporate networks and online services economize on the number of IP addresses they use by sharing a pool of IP addresses among a large number of users.
70. Id. This would involve the use of so-called "fraudulent packets." Id.
71. KLS can be sent to the suspect via e-mail or planted by agents who take advantage of common vulnerabilities to break into a suspect's computer.
72. See Section III.A.1 supra, entitled "Encryption," for a description of how this technology is use to secure communications.
73. See FBI 'Fesses Up to Net Spy App, Reuters (Dec. 12, 2001), available at <www.wired.com /news/conflict/0,2100,49102,00.html>. See Section II.A.2 supra, entitled "Malicious Code," for a description of Trojan horses. The Magic Lantern program is reportedly part of a larger computer surveillance program called "Cyber Knight," which includes a database that allows the FBI to gather evidence from e-mail messages, chat rooms, instant messages, and Internet phone calls.
74. While the United States National Security Agency (NSA) takes the lead, ECHELON works in conjunction with other intelligence agencies, including the Australian Defence Signals Directorate (DSD). It is believed that Echelon also works with Britain's Government Communications Head quarters (GCHQ) and the agencies of other allies of the United States, pursuant to various treaties.
75. On September 5, 2001, the European Union voted 367-159, with 34 abstentions, to adopt 44 recommendations designed to counter ECHELON.
76. In May 2001, a new variant of the LoveLetter worm surfaced that contained a list of words designed to attract the ECHELON system. The worm's code contained a list of almost 300 terms that could trigger surveillance systems.
77. In June 2001, the United States has agreed to share highly classified material from the Anglo-American Echelon intelligence network with the Spanish Government to help Madrid's battle against the Basque separatist group ETA. The deal was alluded to by Mr. Josep Piqué, Spain's Foreign Minister, who confirmed in general terms that the United States had agreed to spy on ETA.
78. U.S. Const., amend IV, available at <caselaw.lp.findlaw.com/data/constitution/amendment04/>.
79. See Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).
80. Id. at 361.
81. See O'Connor v. Ortega, 480 U.S. 709, 715 (1987). For example, the Supreme Court has held that a person has a reasonable expectation of privacy in property located inside a person's home, see Payton v. New York, 445 U.S. 573, 589-90 (1980); in conversations taking place in an enclosed

phone booth, see Katz, 389 U.S. at 358; and in the contents of opaque containers, see United States v. Ross, 456 U.S. 798, 822-23 (1982). In contrast, a person does not have a reasonable expectation of privacy in activities conducted in open fields, see Oliver v. United States, 466 U.S. 170, 177 (1984); in garbage deposited at the outskirts of real property, see California v. Greenwood, 486 U.S. 35, 40-41 (1988); or in a stranger's house that the person has entered without the owner's consent in order to commit a theft, see Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

[82] 389 U.S. 347 (1967).

[83] See Olmstead v. United States, 277 U.S. 438 (1928).

[84] See Pub. L. No. 90-351, 82 Stat. 212.

[85] 18 U.S.C. §§ 2510-22, available at <www4.law.cornell.edu/uscode/18/2510.html>.

[86] See Section III.E supra, entitled "Intercepting Communications," for the practical applications of Title III to the interception of electronic communications. Also see, generally, DOJ Search Manual.

[87] 18 U.S.C. § 2518(4).

[88] Pub.L. 99-508, Oct. 21, 1986, 100 Stat. 1848 (codified in 18 U.S.C. §§ 1367, 2521, 2701 to 2709, 2711, 3117, 3121 to 3124, 3126 and 3127).

[89] This includes electronic communications that are in transit between machines and which contain no aural (i.e., human voice) component. The ECPA also expanded electronic surveillance authority to include telecommunications technologies and services such as electronic mail, cellular telephones, and paging devices. Thus, communications involving computers, faxes, and pagers (other than "tone-only" pagers) all enjoy the broad protections provided by Title III unless one or more of the statutory exceptions to Title III applies. See Section III.E supra, entitled "Intercepting Communications," for an explanation of when such exceptions apply.

[90] Electronic Communications Privacy Act § 102, 100 Stat. at 1853.

[91] See generally 18 U.S.C.A. § 2703 (West 2001). It is possible that this classification reflects the reality that providers available to the public are not likely to have close relationships with their customers, and therefore might have less incentive to protect their customers' privacy.

[92] See Section III.E supra entitled "Intercepting Communications" for a brief description of the procedural safeguards established by Title III and the ECPA.

[93] See Note 118 infra, for a description of an ECPA warrant.

[94] Section 815 of the USA PATRIOT Act amended the ECPA to make clear that the "statutory authorization" defense includes good-faith reliance on a government request to preserve evidence under 18 U.S.C. § 2703(f). The concern that a search executed pursuant to a valid warrant might violate the ECPA derives from Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993). In Steve Jackson Games, the district court held the Secret Service liable under ECPA after it seized, reviewed, and (in some cases) deleted stored electronic communications seized pursuant to a valid search warrant. See id. at 443.

[95] 18 U.S.C. 2701-2711, available at <caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/121/toc.html>.

[96] Courts and scholars have struggled to determine the precise boundaries of and intended relationship between the Wiretap Act and the Stored Communications Act by looking to the language of the statute, legislative history, and a basic understanding of communication technology. See, e.g., Steve Jackson Games 36 F.3d 457; Wesley College v. Pitts, 974 F.Supp. 375 (D. Del. 1997); Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001); Tatsuya Akamine, Proposal for a Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act, 7 J.L. & Pol'y 519, 528 (1999).

[97] The phrase "for purposes of backup protection of such communication" in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of "electronic storage."

[98] "Electronic storage" is defined under the Act as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

[99] 47 U.S.C. 1001 et seq., available at <caselaw.lp.findlaw.com/casecode/uscodes/47/chapters/9/subchapters/i/sections/section_1001.html>.

[100] See Communications Assistance for Law Enforcement Act, CALEA Implementation Section Fed-

eral Bureau of Investigation Report ("CALEA Report"), available at <www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm>.

101. The key terms and phrases of CALEA, such as "call-identifying information," "information services," and "telecommunications carrier," are defined in section 102. Section 103 establishes four assistance capability requirements that telecommunications carriers must meet in connection with services or facilities. Under this section, telecommunications carriers must ensure that they are capable of conducting interceptions and providing access to call-identifying information unobtrusively. Carriers must also protect the privacy and security of communications and call-identifying information not authorized to be intercepted, as well as information about the government's interception of call content and access to call-identifying information.

102. See CALEA Report, supra note 98, (stating that "Congress assigned the Attorney General of the United States a key role in the implementation of CALEA, the most important being that of chief integrator and spokesperson for the law enforcement community").

103. See CALEA Report, supra note 98, (stating that "[c]onsistent with the FCC's duty to regulate the use of wire and radio communications, Congress assigned specific CALEA responsibilities to the FCC"). CALEA also amends the Communications Act of 1934 to provide that the FCC "shall prescribe such rules as are necessary to implement [CALEA]." 47 U.S.C. § 229.

104. See CALEA Report, supra note 98, (stating that "[t]elecommunications carriers must ensure that equipment, facilities, or services that provide customers the ability to originate, terminate, or direct communications meet the [various] assistance capability requirements").

105. See CALEA Report, supra note 98, (stating that "Congress also recognized that without the assistance of manufacturers of telecommunications equipment and support service providers, carriers would be unable to comply with CALEA").

106. See 28 C.F.R. § 0.85 (1995).

107. The CIS website is available at <www.askCALEA.net>.

108. 18 U.S.C. § 3121 et seq., available at <caselaw.lp.findlaw.com/casecode/uscodes/18/parts/ii/chapters/206/toc.html>.

109. See 18 U.S.C. § 3121, available at <caselaw.lp.findlaw.com/casecode/uscodes/18/parts/ii/chapters/206/sections/section_3121.html>.

110. For example, the statute defined "pen register" as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3).

111. This section is not subject to the sunset provision in section 224 of the Act.

112. Section 216 of the USA PATRIOT Act amends sections 3121, 3123, 3124, and 3127 of Title 18 to clarify that the Pen/Trap Statute applies to any non-content information (i.e., dialing, routing, addressing, and signaling information) utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail. Traditionally, pen register or trap-and-trace "devices" were physically attached to the target facility. Due to the fact that this is not necessary for electronic communications, section 216 makes two other related changes. First, due to the fact that such functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen register or trap-and-trace device to be "attached or applied" to the target facility. Likewise, section 216 revises the definitions of "pen register" and "trap and trace device" in section 3127 to include an intangible "process" (such as a software routine) which collects the same information as a physical device.

113. Section 216 of the USA-PATRIOT Act divides 18 U.S.C. 3123 into two separate provisions. New subsection (a)(1) allows federal courts to compel assistance from any U.S. communications services provider whose assistance is appropriate to effectuate the order. The amendments in section 216 of the Act also empower courts to authorize the installation and use of pen/trap devices in other districts. Section 216 of the Act modifies 18 U.S.C. 3123(b)(1)(C) to eliminate the requirement that federal pen/trap orders specify their geographic limits. However, because the new law gives nationwide effect for federal pen/trap orders, an amendment to section 3127(2)(A) imposes a "nexus" requirement: the issuing court must have jurisdiction over the particular crime under investigation.

114. See Section III.B.1 supra entitled "Carnivore."

115. See 18 U.S.C. 2703. Section 210 of the USA PATRIOT Act, which is not subject to section 224's sunset provision, amended section 2703(c) of the ECPA by updating and expanding the list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." Such records include the IP address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Moreover, the amendments clarify that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for his or her account with a communications provider, "including any credit card or bank account number." 18 U.S.C. §2703(c)(2)(F).

116. Courts may authorize law enforcement agencies to install and use a pen register device that identifies the source of calls placed from (outgoing) or a trap-and-trace device that identifies the source of calls to a particular telephone (incoming). The Pen/Trap Statute mandates that such court orders only be provided upon certification that the target information is relevant to a pending criminal investigation and do not require a showing of probable cause. See 18 U.S.C. § 3121(b), available at <caselaw.lp.findlaw.com/casecode/uscodes/18/parts/ii/chapters/206/sections/section_3121.html>. Often, the nature of electronic communications causes addressing information (which does not include the content of the message) to be mixed in with other non-content data. If the service provider can comply with the order and provide the agent with only the addressing information required by the court order, it will typically do so. If, however, the service provider is unwilling or unable to comply with the order, various measures may be pursued by law enforcement. It is for this narrow set of circumstances that the system commonly referred to as "Carnivore" is to be employed. See Statement of Kevin Digregory, Deputy Assistant Attorney General Criminal Division (July 24, 2000), available at <www.cybercrime.gov/carnivore.htm>.

117. A distinction must be made between a search warrant issued under Fed.R.Civ.P. 41 that authorizes law enforcement to execute a search and an ECPA search warrant that compels a provider of electronic communication service or remote computing service to disclose the contents of a subscriber's network account to law enforcement. Although both are called "search warrants," they are very different in practice. ECPA search warrants required by 18 U.S.C. § 2703(a) are court orders that are served much like subpoenas: ordinarily, the investigators bring the warrant to the provider, and the provider then divulges the information described in the warrant to the investigators within a certain period of time. In contrast, Rule 41 search warrants typically authorize agents to enter onto private property, search for and then seize the evidence described in the warrant. This distinction is especially important when a court concludes that ECPA was violated and then must determine the remedy. Because the warrant requirement of 18 U.S.C. § 2703(a) is only a statutory standard, a non-constitutional violation of § 2703(a) should not result in suppression of the evidence obtained.

118. See Section III.C supra, entitled "Statutory Framework," for a review of Title III and the ECPA.

119. The application must also provide additional detail, including whether there have been previous interceptions of communications of the target, the identity of the target (if known), the nature and location of the communications facilities, and a description of the type of communications sought and the offenses to which the communications relate. By statute and internal Department regulation, the interception may last no longer than thirty days without an extension by the court. Courts also often impose their own requirements. For example, many federal courts require that the investigators provide periodic reports setting forth information such as the number of communications intercepted, steps taken to minimize irrelevant traffic, and whether the interceptions have been fruitful. The court may, of course, terminate the interception at any time.

120. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

121. See 18 U.S.C. § 2707(e); Davis v. Gracey, 111 F.3d 1472, 1484 (10th Cir. 1997) (applying good faith defense because seizure of stored communications incidental to a valid search was objectively reasonable). Cf. Steve Jackson Games, 816 F. Supp. at 443 (stating without explanation that the court "declines to find this defense").

122. See Illinois v. Andreas, 463 U.S. 765, 771 (1983).

123. See Illinois v. Rodriguez, 497 U.S. 177, 183 (1990).

124. Other exceptions include communications intercepted in the ordinary course of business and the interception of publicly accessible communications. See 18 U.S.C. 2511(g)(i), available at <caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/119/sections/section_2511.html>

(stating that "It shall not be unlawful ... for any person ... to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." "Available to the public" has been interpreted as communications that are not encrypted and not password protected.).

125. 18 U.S.C. § 2511(2)(c).

126. See United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993); also see United States v. Seidlitz, 589 F.2d 152, 158 (4th Cir. 1978). Under new Section 2511(2)(i), which will sunset December 31, 2005, law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met:
1) Section 2511(2)(i)(I) requires that the owner or operator of the protected computer must authorize the interception of the trespasser's communications;
2) Section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation;
3) Section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation; and
4) Section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

127. If the communication merely passes through a victim's computer, however, a court may be hesitant to conclude that the victim computer is a "party" to the communication. In this scenario, the victim's computer is merely receiving electronic communications and passing them on to downstream victims and/or confederates of the subject programmer. While monitoring this downstream traffic is possible, it is debatable whether the victim is in fact a "party to the communication" if the communications are simply passing through its system. A court, therefore, may conclude that the owner is not a "party" capable of giving consent to keystroke monitoring given its pass through role. The statutory exception requires that the new victim give "prior consent" to the monitoring, which will be unlikely in the short term where the victim or victims cannot be known in advance.

128. 18 U.S.C. § 2511(2)(d).

129. Computer networks frequently make use of computer banners that appear whenever a person logs onto the network. A banner is a program that is installed to appear whenever a user attempts to enter a network from a designated point of entry known as a "port." Banners typically inform the user that: (a) the user is on a private network; and (b) by proceeding, the user is consenting to all forms of monitoring.

130. 18 U.S.C. § 2511(2)(a)(i). Also see Section IV.C infra, entitled "Voluntary Disclosures," discussing when providers may disclose the fruits of their discoveries to law enforcement.

131. It is difficult to determine whether a victim has the right to monitor communications made by hackers who merely pass through computer systems without intending to cause damage. Analysis of this situation will depend on how courts interpret the breadth of existing statutory exceptions to Title III. This raises the concern that system trespassers may receive certain statutory protections under Title III. Although no court has explored what this limitation means in the computer context, courts may analogize cases where telephone companies have been prevented from monitoring all the conversations of a user of an illegal clone phone unrelated to the protection of its service. See McClelland v. McGrath, 31 F. Supp.2d 616 (N.D. Ill. 1998).

132. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

133. See id. Although most private search issues arise when private third parties intentionally examine property and offer evidence of a crime to law enforcement, the same framework applies when third parties inadvertently expose evidence of a crime to plain view. For example, in United States v. Procopio, 88 F.3d 21 (1st Cir. 1996), a defendant stored incriminating files in his brother's safe. Later, thieves stole the safe, opened it, and abandoned it in a public park. Police investigating the theft of the safe found the files scattered on the ground nearby, gathered them, and then used them against the defendant in an unrelated case. The First Circuit held that the use of the files did not

violate the Fourth Amendment, because the files were made openly available by the thieves' private search. See id. at 26-27 (citing Jacobsen, 466 U.S. at 113).

134. See 18 U.S.C. §§ 2701-11, discussed in Section III.C.4 supra, entitled "Stored Communications Act."
135. 142 F.3d 988 (7th Cir. 1998).
136. See id. at 993. See also United States v. Kennedy, 81 F. Supp.2d 1103, 1112 (D. Kan. 2000) (concluding that searches of defendant's computer over the Internet by an anonymous caller and employees of a private ISP did not violate Fourth Amendment because there was no evidence that the government was involved in the search).
137. Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (1989).
138. Id. at 614-15 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).
139. See, e.g., United States v. Pervaz, 118 F.3d 1, 6 (1st Cir. 1997); United States v. Smythe, 84 F.3d 1240, 1242-43 (10th Cir. 1996); United States v. McAllister, 18 F.3d 1412, 1417-18 (7th Cir. 1994); United States v. Malbrough, 922 F.2d 458, 462 (8th Cir. 1990).
140. See, e.g., United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982) (holding that private action counts as government conduct if, at the time of the search, the government knew of or acquiesced in the intrusive conduct, and the party performing the search intended to assist law enforcement efforts); United States v. Paige, 136 F.3d 1012, 1017 (5th Cir. 1998) (same); United States v. Lambert, 771 F.2d 83, 89 (6th Cir. 1985) (holding that a private individual is a state actor for Fourth Amendment purposes if the police instigated, encouraged or participated in the search, and the individual engaged in the search with the intent of assisting the police in their investigative efforts).
141. The system administrator's job is to keep the network running smoothly, monitor security, and repair the network when problems arise. System operators have "root level" access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems.
142. See Section III.E.1 supra, entitled "Consent of a Party Acting 'Under Color of the Law,'" for a discussion of this exception to the statutory protections relating to such scenarios.
143. See 18 U.S.C. § 2702-03.
144. All of the changes under this Section will sunset December 31, 2005.
145. See 18 U.S.C. 3702(b)(6), available at <caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/121/sections/section_2702.html>.
146. See Section III.E.3 supra entitled "Protecting Provider's Rights and Property" for a discussion of when Service Providers may seek the assistance of law enforcement to monitor their systems.
147. 466 U.S. 109 (1984).
148. Id. at 115. See also United States v. Miller, 152 F.3d 813, 815-16 (8th Cir. 1998); United States v. Donnes, 947 F.2d 1430, 1434 (10th Cir. 1991). But see United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1999) (dicta) (stating that Jacobsen does not permit law enforcement to reenact a private search of a private home or residence).
149. See United States v. Barth, 26 F. Supp.2d 929, 937 (W.D. Tex. 1998) (suppressing evidence of child pornography found on computer hard drive after agents viewed more files than private technician had initially viewed during repair of defendant's computer).
150. Netwar Revisited at p. 15.
151. See Computer Emergency Response Team Report, Carnegie Mellon University (Mar. 2001) (stating that attacks on web sites increased from 2,000 in 1997 to 21,000 in 2000; web site defacements totaled 5,000 in 2000, up from just five in 1995; and viruses were up 20 percent in 2000).
152. The Cybersecurity Research and Development Act would allocate more than $560 million to the National Science Foundation. The foundation would administer grants for educational programs and basic research on computer security techniques and technologies, including authentication, encryption, intrusion detection, reliability, privacy, and confidentiality.
153. In October 2001, the Bush administration backed bipartisan legislation aimed at limiting government disclosures about hack attacks.
154. According to a report released in March 2001 by the Computer Security Institute and the FBI, more companies are beginning to report cybercrime.
155. The U.S. government has pulled information relating to energy production, chemical plants, and pipeline mapping systems from agency Web sites.
156. In April 2001, the Computer Emergency Response Team (CERT) Coordination Center and the

Electronic Industries Alliance announced the "Internet Security Alliance," which will provide threat reports, risk management strategies and security best practices for its members. Also, Microsoft, together with five security companies, announced they plan to form a group that will devise policies and guidelines for responsible vulnerability disclosure.

157. See Brian Whitaker, US Pulls the Plug on Muslim Websites, BBC News (Sep. 10, 2001) (reporting that five hundred websites—many of them with an Arab or Muslim connection—reportedly crashed when an anti-terrorism taskforce raided InfoCom Corporation in Texas).
158. See the National Institute of Technology Standards (NIST) web site, available at <csrc.nist.gov/encryption/aes/>, stating that the U.S. government updated its encryption standard for computer transmissions in December 2001, replacing an aging standard first put in place in 1977 with the 256 Bit Advanced Encryption Standard (AES).
159. See Michelle Delio, GovNet: What is it Good For?, Wired (Jan. 21, 2002) (stating that the Bush Administration's Special Advisor for Cyberspace Security, Richard Clarke, proposed the formation of a new network that would exclusively be used to transfer sensitive government information and has been dubbed "GOVNET"), available at <www.wired.com/news/politics/0,1283,49858,00.html>.
160. See Press Release (Oct. 17, 2001) (stating that Governor James Gilmore (R-Virginia), leader of the Office of Homeland Security, recommended that Congress create a cyber court to exercise over sight in the investigation of suspected computer criminals), available at <www.house.gov/science/press/107pr/107-103.htm>.
161. On October 9, 2001 President Bush appointed Richard Clarke, a coordinator of security for the National Security Council, as his special advisor for cyberspace security. See Richard A. Clark Biography, available at <www.fpc.gov/admin/clarke.htm>. Clarke will report to National Security Advisor Condoleezza Rice and to newly appointed Director of Homeland Defense, Tom Ridge.
162. See Executive Order on Critical Infrastructure Protection (Oct. 16, 2001) ("Critical Infrastructure Order") (providing that "the Board shall recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems"), available at <www.whitehouse.gov/news/releases/2001/10/20011016-12.html>.
163. The Critical Infrastructure Order states that the National Infrastructure Advisory Council is an advisory body made up of representatives of the private sector, academia, and state and local government. The Council is to "provide the President advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services."
164. See FBI Reorganization Chart, available at <www.fbi.gov/pressrel/eads/chart.htm>, and FBI Press Release (Dec. 3, 2001), available at <www.fbi.gov/pressrel/pressrel01/reorg120301.htm>.
165. OHS is led by Governor James Gilmore (R-Virginia) and its web site is located at <www.homelandsecurity.org>.
166. The adjective "white hat" is used to describe hackers who identify security weaknesses in computer systems or networks. Instead of taking malicious advantage of the weakness, however, the white hat hacker exposes the weakness in a way that will allow the system's owners to fix the breach before it is can be taken advantage by others (such as "black hat" hackers). See note 12 supra for a description of the terms "hacker" and "cracker."
167. <www.cultdeadcow.com/>.
168. <www.microsoft.com/ms.htm>.
169. See James Middleton, Infamous Hacker Group Helps the Feds, Vnunet.com (Dec. 12, 2001) available at <www.vnunet.com/News/1127639>. See Section III.B.2, entitled "Keyboard Logging Systems," for a review of such systems.
170. This presents novel legal questions regarding search and seizure and credibility. For instance, the use of such viral infiltration raises the question of who in fact conducted the search and whether the gathered information would simply be treated as a typical anonymous source. It also raises questions as to whether the subject of the search would have civil claims based on the search and, if so, against whom and for what?
171. See Section III.A.1 supra, entitled "Encryption," for a description of government attempts to create a backdoor to encryption accounts.
172. See Shawna McAlearney, FBI Admits Existence of "Magic Lantern," Information Security (Dec. 3,

2001). Officials at Symantec Corp. and Network Associates Inc. however, subsequently stated that they had no intention of voluntarily modifying their products to satisfy the FBI. Also see Section II.A.4, entitled "Security Measures," for a description of anti-virus software and Section II.A.2, entitled "Malicious Code," for a description of Trojans.

173. See Michelle Delio, A Chinese Call to Hack U.S., Wired (April 11, 2001), available at <www.wired.com/news/politics/0,1283,42982,00.html>. This is not this first instance of China-based attacks to the U.S. National Infrastructure. See Robert O'Harrow, Jr., Key U.S. Computer Systems Called Vulnerable to Attack, Wash. Post (Sept. 27, 2001, available at <www.washingtonpost.com/ac2/wp-dyn/A32105-2001Sep26>.

174. See Michele Delio, Crackers Expand Private War, Wired (Apr. 18, 2001), available at <www.wired.com/news/politics/0,1283,43134,00.html>.

175. <www.hacktivismo.com/>. Hacktivismo reportedly grew out of the Cult of the Dead Cow (cDc), a team of white-hat hackers best known for producing security tools that exploit weaknesses in Microsoft software. The cDc has created such tools as BackOrifice and BackOrifice2000, which allow a computer hacker to take control of computers running Microsoft operating systems.

176. See Warren Allmand, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China (stating that China seeks to replace "traditional" censorship with a massive, ubiquitous architecture of surveillance called the "Golden Shield"), available at <www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html>.

177. See Section III.A.2 supra, entitled "Anonymizing Technology," for a discussion of anonymous networks.

178. Peekabooty is reportedly based on peer-to-peer network technology to allow data to be distributed directly between computer systems. Peekabooty hosts cooperate in a similar way to Gnutella—without a central server—to enable distribution of controversial Web pages.

179. See Section III.C.1 supra, entitled "Fourth Amendment," for a discussion of the privacy principles established by Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).

180. For instance, government agencies can create "mirror" sites that encourage hackers to penetrate and share results. Also, hacktivism may take many forms, from intelligence agents who penetrate a hostile nation's computer system to gather intelligence, system administrators who monitor net works for suspicious activity, or a private user who secures systems from criminal enterprises through the use of firewalls.

181. See Hackers Take Up Larry Ellison's Challenge, USA Today (Dec. 10, 2001) (stating that Oracle's "Unbreakable" ad campaign, challenging hackers everywhere to try to break into the company's servers, has met with resounding success by increasing the security of such products), available at <www.usatoday.com/life/cyber/tech/2001/12/10/oracle-hackers-challenge.htm>.