Hacktivism: Securing the national infratructure

Milone, Mark G . The Business Lawyer ; Chicago Vol. 58, Iss. 1, (Nov 2002): 383-413.

ABSTRACT

Modern society is increasingly dependent on networked computer systems to facilitate its critical functions. This complex architecture, the central nervous system of the United States' "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 the National Infrastructure and counter networked crime and terrorism. An overview of some of the common techniques used to access and/or damage computer systems is presented. The laws and regulations governing computer crimes, including the Computer Fraud and Abuse Act, are also discussed. Technology features and tools that can enhance privacy and security, as well as surveillance technology that can be used to catch cybercriminals, are explained. The implications of these tools as they apply to search and seizure and right of privacy are discussed at length.

FULL TEXT

INTRODUCTION

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.

NATIONAL INFRASTRUCTURE

The National Infrastructure is composed of "critical systems" that 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 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., "networking"), the

nervous systems of living creatures (i.e., "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 militant groups where everybody is connected to everybody else) .6
One can see that a full matrix network, such as cyberspace, presents the most efficient and resilient communications architecture. Cyberspace, however, is subject 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)7 and the number of interconnections between nodes.8 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.9 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.10

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."11 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."12 A hacktivist, therefore, uses the same tools and techniques as a hacker,13 but does so in order to bring attention to a larger, political or social goal.14 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."15 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.16

TECHNOLOGY AND TARGETS

Each computer that is connected to cyberspace is susceptible to intrusion. Most computer criminals, 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.17 The following is a brief overview of some of the common techniques used to access and/or damage computer systems.

Unauthorized Access

System crackers typically use cyberspace to access computer systems via "ports," which act as points of entry into the network.18 Computer systems are designed to have hundreds of ports for different types of uses such as electronic mail, remote login, or telnet. Most of these ports are not in use and remain closed, and can only be opened by a system administrator. Intruders 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.19

Malicious Code

Programmers may also create and distribute malicious code (also called "malware") such as viruses,20 Trojan horses,21 and worms22 in order to cause potentially global computer damage.23 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 code is activated.24

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.25 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.26

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, that protects the resources of a private network from users from other networks."27 A firewall may also be used to control the outside resources to which network users have access.28 Anti-virus software, on the other hand, searches computer systems for any known or potential viruses.

THE COMPUTER FRAUD AND ABUSE ACT29

Computer crimes are primarily addressed by the Computer Fraud and Abuse Act (CFAA).30 The CFAA makes it unlawful for any person to access a protected computer 31 "without authorization."32 It also forbids a person who has a legitimate and authorized right of access from "exceeding [the] authorized access."33 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 software34 and trafficking in stolen passwords.35 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.36

THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ACT OF 2001(37)

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.38 In essence, the USA PATRIOT Act seeks to protect the National Infrastructure by easing the restrictions placed on electronic surveillance39 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."40 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, individuals in foreign countries frequently routed communications through the United States as they hack from one foreign country to another. In such cases, the lack of any U.S. victim discouraged U.S. law enforcement agencies from assisting any foreign investigation or prosecution.

Section 814 of the USA PATRIOT Act amends the definition of "protected computer"41 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."42 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 of 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,43 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.44 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.45 Amendments in section 814 codify the broad definition of "loss" adopted in Middleton.46

Aggregating Damages

Prior to the USA PATRIOT Act's amendments, 18 U.S.C. sec 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.47

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, an individual 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 of 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.48

Clarification of Intent To Cause Damage

Under previous law, in order to violate 1030(a)(5)(A), an offender had to "intentionally [cause] damage without authorization."49 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.50 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."51 An actor will violate sec 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.52

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 of 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 sec 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.(53)

Raising Penalties and Eliminating Mandatory Minimums

Under previous law, first-time offenders who violate sec 1030(a)(5) could be punished by no more than five years' imprisonment, while repeat offenders could receive up to ten years.54 Certain offenders, however, can cause severe damage to protected computers and it was argued that this five-year maximum did not adequately take into account the seriousness of their crimes.55 In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of sec 1030(a)(5), as well as for violations of sec 1030(a)(4) .56 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.57 Congress chose to eliminate all mandatory minimum guidelines sentencing for sec 1030 violations. New legislation has also been introduced to further increase these penalties.58

GOVERNMENT SEARCH AND SEIZURE59

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 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 these 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.60 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.61

Encryption

Encryption (also called "cryptography") is used to secure information by converting data into "ciphertext" so that it in not easily understood by unauthorized people.62 Encryption generally contains two components:

Cryptography: the improvement of methods for keeping data secure from unauthorized parties, and63

Cryptanalysis: the circumvention of cryptographic codes.64

There are many products available for users to utilize encryption technology.65 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.66

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 innovations67 or by requiring "backdoors," called "government escrow,"68 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 concomi

tantly strengthens criminal cryptanalysis and destabilizes intellectual and/or financial property.69

Anonymizing Technology

There is a wide spectrum of competency and motives amongst people who want their online identity to remain hidden.70 Anonymous networks provide one of the most comprehensive forms of anonymity in electronic communications. Anonymous networks exist 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,71 an open-source project viewed by many as the successor to Napster's original promise of free online file swapping.71

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.73 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.74 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.75 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.76 Carnivore is reportedly subject to several technical deficiencies.77 For instance, problems may arise while attempting to track dynamically assigned IP addresses.78 Also, "[t] here is a question of whether Carnivore could distinguish real network traffic versus traffic generated to trick the technology."79

Keyboard Logging Systems

Keyboard Logging Systems (KLS) use remotely installed software to capture the keystrokes of suspected criminals and transmit this information to agents in real time.80 By tracking exactly what a suspect types, encryption key information can be gathered and transmitted back to law enforcement.81 For example, under a project named "Magic Lantern," the Federal Bureau of Investigations (FBI) allegedly created a Trojan horse to facilitate KLS infiltration of suspect computer systems82 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.83 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 everyday, 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 systems84 and code designed to attract the attention of the ECHELON system.85 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.86

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. secs 2510-2522, 2701-2711, and 3121-3127 and 47 U.S.C. secs 1001 et seq. Although constitutional and statutory issues overlap in some cases, most surveillance presents either a constitutional issue under the Fourth Amendment or a statutory issue under these four statutes.

Fourth Amendment87

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.88 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.'"89 No bright line rule indicates whether an expectation of privacy is constitutionally reasonable.90 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.91 Prior to Katz, the Supreme Court had regarded wiretapping as outside the scope of the Fourth Amendment's restrictions on unreasonable searches and seizures.92 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.93 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.94

Wiretap Act95

The Wiretap Act, commonly known as Title III, prohibits the intentional interception of any "wire, oral or electronic communication."96 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."97

Electronic Communications Privacy Act of 1986(98)

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.99 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.100

The ECPA classifies electronic communications according to privacy interests that are implicated by the information sought.101 For example, disclosure of stored e-mails involves a different privacy interest than providing subscriber account information.102 The ECPA also subjects computing services available "to the public" to more strict regulation than services that are not available to the public.103 To protect these privacy interests, the ECPA offers varying degrees of legal protection depending on the perceived seriousness of the privacy interest involved.104 With certain exceptions, the ECPA criminalizes and creates civil liability for intentionally intercepting electronic communications without a judicial warrant.105 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.106

Stored Communications Act107

The Stored Communications Act, Title II of the ECPA, provides protection for messages while they are in the course of transmission.108 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.109 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 ...."110 The Stored Communications Act, therefore, does not apply to messages acquired after

transmission to the intended recipient is complete.

Communications Assistance for Law Enforcement Act111

Since 1970, telecommunications carriers have been required to cooperate with law enforcement personnel in conducting lawfully authorized electronic surveillance.112 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.113 CALEA also imposes certain responsibilities on the Attorney General of the United States,114 the Federal Communications Commission (FCC),115 telecommunications equipment manufacturers,116 and telecommunications support services providers.117 On February 24, 1995, the Attorney General delegated management and administrative responsibilities for CALEA to the FBI.118 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.119

Pen Register and Trap-and-Trace Statute 120

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.121 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.122 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 Act123 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;124

2. Pen/trap orders issued by federal courts have nationwide effect;125 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.126

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,127 a court order to obtain transactional records identifying the source and destination of communications,128 a warrant to obtain the actual content of

electronic communications,129 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.130 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.131 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.132 Objectively reasonable good faith reliance on a warrant, court order, or statutory authorization is a complete defense to such violations.133

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 "legitimate expectation of

privacy," then formally it does not constitute a Fourth Amendment "search" and no warrant is required.134 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.135 Three common exceptions exist.136 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."137 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.138 Under this exception, therefore, it has been held that a victim may monitor, and authorize the government to monitor, hacking activity directly with his or her computer.139

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."140 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.141 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 carrier of that service."142 This exception allows private parties to monitor their system to prevent misuse. Because network intrusion often involves damage or disabling of a network's computer security system, as well as theft of the networks 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 hacking activities on other networks. This limitation also makes it difficult for a network administrator to justify monitoring hacking activities when the subject jumps to a new downstream victim.143

PRIVATE SEARCH AND 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 govemmental official.'"144 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.145 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.146

In United States v. Hall,147 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.148

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."149 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.'"150

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.151

Other circuits have adopted more rule-like formulations that focus on only certain aspects of these factors. 152

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.153

As a practical matter, the primary barrier to searching a network account pursuant to a system administrator's consent is statutory, not constitutional.154 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.155 Accordingly, any attempt to obtain a system administrator's consent to search an account must comply with the ECPA. To the extent that the 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 Act156 amended sec 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.157 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. 158 First, amendments to secs 2702 and 2703 of Title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to sec 2702.(159)

Thus, sec 2702 now regulates all permissive disclosures of content and non-content records alike, while sec 2703 covers only compulsory disclosures by providers. 160 Second, an amendment to new sec 2702(c)(3) clarifies that service providers have the statutory authority to disclose non-content records to protect their rights and property.161

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,162 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."163 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. As soon as agents exceed the scope of the private warrantless search, however, any evidence uncovered may be suppressed.164

LOOKING FORWARD

"It takes networks to fight networks."165 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.166 Recent measures include:

1. Allocating funds to increase the resilience of the National Infrastructure;167
2. Introducing legislation to limit government disclosure of successful attacks;168
3. "Encouraging" private parties to share information relating to successful attacks;169
4. Removing certain information from government Web sites;170
5. Forming governmental-corporate alliances;171
6. Disabling suspected terrorist-supported Web sites; 172
7. Updating government encryption standards; 173 and
8. Proposing government-only networks174 and cybercrime-specific courts.175

Taking the lead in securing the National Infrastructure are the Bush Administration's Special Advisor for Cyberspace Security,176 Critical Infrastructure Protection Board (CIPB)177 and National Infrastructure Advisory Counsel (NIAC),178 the newly reorganized FBI,179 and the Office of Homeland Security (OHS).180

GOVERNMENT ALLIANCES

Private industry and "white hat" hackers181 have begun to offer up their services to the government through various initiatives. For instance, the Cult of the Dead Cow (cDc)182 and Microsoft183 have both reportedly offered assistance to the FBI's Magic Lantern initiative, which was used to develop the FBI's keyboard logging software.184 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.185

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,186 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.187 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.188 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.(189) Another hacktivist group, Hacktivismo,190 responded to China's alleged censorship initiatives entitled "the Great Firewall of China" and "the Golden Shield"191 through the creation of software called "Peekabooty." Much like anonymous networks,192 Peekabooty allegedly enables individuals living in oppressive regimes to access prohibited material through fellow Peekabooty clients located in more liberal countries.193

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 timetested constitutional principle of privacy. If law enforcement fails properly to 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.194 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 computerrelated 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 hacktivism195 and fuel hacktivists' innate love of a good challenge.196

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.

AuthorAffiliation

By Mark G. Milone*

AuthorAffiliation

*Mark G. Milone is Associate General Counsel at the New York Mercantile Exchange (http:// www.nymex.com) and a graduate of Hofstra University School of Law (http://www.hofstra.edu/law). if you have any questions or comments, Mr. Milone can be reached at milone@mindspring.com. This Article does not necessarily reflect the views of the New York Mercantile Exchange.

DETAILS

Subject:	Computer security; Network security; Constitutional law; National security; Computer crime
Location:	United States US
Classification:	9190: United States; 5220: Information technology management; 5140: Security management; 4300: Law
Publication title:	The Business Lawyer; Chicago
Volume:	58
Issue:	1
Pages:	383-413
Number of pages:	31
Publication year:	2002
Publication date:	Nov 2002
Publisher:	American Bar Association
Place of publication:	Chicago
Country of publication:	United States, Chicago
Publication subject:	Business And Economics, Law--Corporate Law
ISSN:	00076899
e-ISSN:	21641838
Source type:	Trade Journals
Language of publication:	English

Document type:	Feature
ProQuest document ID:	228453856
Document URL:	http://argo.library.okstate.edu/login?url=https://search.proquest.com/docview/228453856?accountid=4117
Copyright:	Copyright American Bar Association, Section of Business Law Nov 2002
Last updated:	2016-03-27
Database:	ABI/INFORM Collection,Research Library

LINKS

Link to Full Text