Prosecuting Computer Crimes

Michael Battle
Director, EOUSA

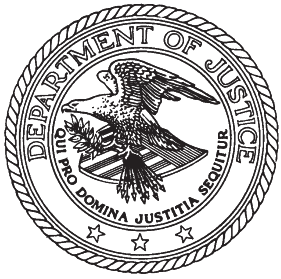
Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director, OLE

Scott Eltringham
Computer Crime and Intellectual Property Section
Editor in Chief

Computer Crime and Intellectual Property Section
Criminal Division



Published by
Office of Legal Education
Executive Office for
United States Attorneys

Table of Contents

Preface and Acknowledgements v

Chapter 1. Computer Fraud and Abuse Act 1
A. Key Definitions 3
B. Obtaining National Security Information ..... § 1030(a)(1) 10
C. Compromising Confidentiality ..... § 1030(a)(2) 15
D. Trespassing in a Government Computer ..... § 1030(a)(3) 19
E. Accessing to Defraud and Obtain Value ..... § 1030(a)(4) 22
F. Damaging a Computer or Information ..... § 1030(a)(5) 29
G. Trafficking in Passwords ..... § 1030(a)(6) 46
H. Threatening to Damage a Computer ..... § 1030(a)(7) 49
I. Legislative History 51

Chapter 2. Wiretap Act 55
A. Intercepting a Communication ..... § 2511(1)(a) 56
B. Disclosing an Intercepted Communication ..... § 2511(1)(c) 63
C. Using an Intercepted Communication ..... § 2511(1)(d) 66
D. Statutory Exceptions 67
E. Defenses 74
F. Statutory Penalties 74

Chapter 3. Other Network Crime Statutes 77
A. Unlawful Access to Stored Communications ..... § 2701 77
B. Identity Theft ..... § 1028(a)(7) 84
C. Aggravated Identity Theft ..... § 1028A 85
D. Access Device Fraud ..... § 1029 85
E. CAN-SPAM Act ..... § 1037 86
F. Wire Fraud ..... § 1343 90
G. Communication Interference ..... § 1362 91

Chapter 4. Special Considerations 93
A. Jurisdiction 93
B. Venue 95
C. Statute of Limitations 99
D. Juveniles 99

Chapter 5. Sentencing 109
A. Base Offense Levels 109
B. Adjustments Under Section 2B1.1 110
C. CAN-SPAM Act 121
D. Wiretap Act 121
E. Generally-Applicable Adjustments 122
F. Conditions of Supervised Release 124

Appendices
A. Unlawful Online Conduct and Applicable Federal Laws 127
B. Best Practices for Working with Companies 135
C. Best Practices for Victim Response and Reporting 139
D. Network Crime Resources 147

Index 151

Preface and Acknowledgements

This manual is a product of the Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice. Just as in *Searching and Seizing Computers and Electronic Evidence* (2d ed. 2002) and *Prosecuting Intellectual Property Crimes* (3d ed. 2006), we emphasize real world practice issues for working prosecutors.

This manual examines the federal laws that relate to computer crimes. Our focus is on those crimes that use or target computer networks, which we interchangeably refer to as "computer crime," "cybercrime," and "network crime." Examples of computer crime include computer intrusions, denial of service attacks, viruses, and worms. We make no attempt to cover issues of state law and do not cover every type of crime related to computers, such as child pornography or phishing.

We refer to people committing the crimes covered in this manual as "intruders" or "attackers" instead of the more widely-used but less-specific term "hackers."

This manual is a joint effort of the Computer Crime team of CCIPS, under the supervision of Martha Stansell-Gamm, Chief, and Christopher Painter, Principal Deputy Chief. Scott Eltringham is the primary editor, but this manual exists because of the work and experience of many CCIPS attorneys, both present and former, including Leonard Bailey, Howard Cox, Richard Downing, Tom Dukes, Josh Goldfoot, Jessica Herrera, Todd Hinnen, Amanda Hubbard, Nathan Judish, Kimberly Peretti, Richard Salgado, Jared Strauss, Joel Schwarz, Betty Shave, Joe Springsteen, Michael Stawasz, Michael Sussmann, Anthony Teelucksingh, Eric Wenger, Lisa Willmer, and William Yurek, paralegals Kathleen Baker and Aubrey Rupinta, as well as many of our legal interns.

We are grateful to Ed Hagen, Nancy Bowman, and others at the Office of Legal Education for their assistance in publishing this manual.

This manual is intended as assistance, not authority. The research, analysis, and conclusions herein relect current thinking on difficult and dynamic areas of the law; they do not represent the official position of the Department of Justice or any other agency. This manual has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S. Department of Justice directive. *See United States v. Caceres*, 440 U.S. 741 (1979).

If you have questions about anything in this manual, we invite you to call CCIPS at (202) 514-1026. Attorneys are on duty every day for the specific purpose of answering such calls and providing support to U.S. Attorneys' offices, law enforcement agencies, and other public- and private-sector partners.

Electronic copies of all three of our manuals are available at http://www.cybercrime.gov. The electronic version will be periodically updated, and prosecutors and agents are advised to check the website for the latest developments.

John T. Lynch, Jr.
Deputy Chief
Computer Crime & Intellectual Property Section
Criminal Division
Department of Justice

Chapter 1
Computer Fraud and Abuse Act

In the early 1980s law enforcement agencies faced the dawn of the computer age with growing concern about the lack of criminal laws available to fight the emerging computer crimes. Although the wire and mail fraud provisions of the federal criminal code were capable of addressing some types of computer-related criminal activity, neither of those statutes provided the full range of tools needed to combat these new crimes. *See* H.R. Rep. No. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692.

In response, Congress included in the Comprehensive Crime Control Act of 1984 provisions to address the unauthorized access and use of computers and computer networks. The legislative history indicates that Congress intended these provisions to provide "a clearer statement of proscribed activity" to "the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access." *Id.* Congress did this by making it a felony to access classified information in a computer without authorization, and a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer. In so doing, Congress opted not to add new provisions regarding computers to existing criminal laws, but rather to address federal computer-related offenses in a single, new statute, 18 U.S.C. § 1030.

Even after enacting section 1030, Congress continued to investigate problems associated with computer crime to determine whether federal criminal laws required further revision. Throughout 1985, both the House and the Senate held hearings on potential computer crime bills, continuing the efforts begun in the year before. These hearings culminated in the Computer Fraud and Abuse Act (CFAA), enacted by Congress in 1986, which amended 18 U.S.C. § 1030.

In the CFAA, Congress attempted to strike an "appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses." *See* S. Rep. No. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482. Congress addressed federalism concerns in the CFAA by limiting federal jurisdiction to

cases with a compelling federal interest—i.e., where computers of the federal government or certain financial institutions are involved, or where the crime itself is interstate in nature. *See id*.

In addition to clarifying a number of the provisions in the original section 1030, the CFAA also criminalized additional computer-related acts. For example, Congress added a provision to penalize the theft of property via computer that occurs as a part of a scheme to defraud. Congress also added a provision to penalize those who intentionally alter, damage, or destroy data belonging to others. This latter provision was designed to cover such activities as the distribution of malicious code and denial of service attacks. Finally, Congress also included in the CFAA a provision criminalizing trafficking in passwords and similar items.

As computer crimes continued to grow in sophistication and as prosecutors gained experience with the CFAA, the CFAA required further amendment, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, and 2002. While this manual does not explore each of these amendments, several are discussed in the context of the "Key Definitions" and "Legislative History" sections below. Analysis of the most significant amendments—the National Information Infrastructure Protection Act of 1996 and the USA PATRIOT Act of 2001—are on the CCIPS website, http://www.cybercrime.gov.

The current version of the CFAA includes seven types of criminal activity, outlined in Table 1 below. Attempts to commit these crimes are also crimes. 18 U.S.C. § 1030(b). Lawfully authorized activities of law enforcement or intelligence agencies are explicitly excluded from coverage of section 1030. 18 U.S.C. § 1030(f).

Table 1. Summary of CFAA Provisions

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Compromising the Confidentiality of a Computer	(a)(2)	1 or 5
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Knowing Transmission and Intentional Damage	(a)(5)(A)(i)	10 (20 or life)
Intentional Access and Reckless Damage	(a)(5)(A)(ii)	5 (20)
Intentional Access and Damage	(a)(5)(A)(iii)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Threats to Damage Computer	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parenthesis.

In some circumstances, the CFAA allows victims who suffer specific types of loss or damage as a result of a violations of the Act to bring civil actions against the violators for compensatory damages and injunctive or other equitable relief. 18 U.S.C. § 1030(g). This manual does not address the civil provisions of the statute except as they may pertain to the criminal provisions.

A. Key Definitions

Two terms are common to most prosecutions under section 1030 and are discussed below: "protected computer" and "authorization." Other terms are discussed with their applicable subsection.

1. Protected Computer

The term "protected computer," 18 U.S.C. § 1030(e)(2), is a statutory term of art that has nothing to do with the security of the computer. In a nutshell, "protected computer" covers computers used in interstate or foreign commerce (e.g., the Internet) and computers of the federal government and financial institutions.

"Protected computer" did not appear in the CFAA until 1996, when Congress attempted to correct deficiencies identified in earlier versions of the statute. In 1994, Congress amended the CFAA so that it protected any "computer used in interstate commerce or communication" rather than a "Federal interest computer." This change expanded the scope of the Act to include certain non-government computers that Congress deemed deserving of federal protection. *See* S. Rep. No. 104-357, at 10 (1996), *available at* 1996 WL 492169 (discussing 1994 amendment). In doing so, however, Congress "inadvertently eliminated Federal protection for those Government and financial institution computers not used in interstate commerce." *United States v. Middleton,* 231 F.3d 1207, 1212 n.2 (9th Cir. 2000) (*citing* S. Rep. No. 104-357).

Congress corrected this error in the 1996 amendments to the CFAA, which 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." 18 U.S.C. 1030(e)(2) (1996). The definition did not explicitly address situations where an attacker within the United States attacks a computer system located abroad. In addition, this definition was not readily applicable to situations in

which individuals in foreign countries routed communications through the United States as they hacked from one foreign country to another.

In 2001, the USA PATRIOT Act amended the definition of "protected computer" to make clear 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." 18 U.S.C. § 1030(e)(2)(B) (2001). As a result of this amendment, a protected computer is now defined as a computer "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government" or a computer "used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2).

2. Without or In Excess of Authorization

Many of the criminal offenses contained within the CFAA require that an intruder either access a computer without authorization or exceed authorized access. The term "without authorization" is not defined in the Act and one court found its meaning "to be elusive." *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001) (dicta); *see also SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593 (E.D. Va. 2005) (holding that defendants had authorization to use a computer system even though such access violated the terms of a license agreement binding the user who provided them with access to the system).

The term "exceeds authorized access" is defined by the CFAA to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The legislative history of the CFAA reflects an expectation by Congress that persons who exceed authorized access are likely to be insiders, whereas persons who act without authorization are likely to be outsiders. As a result, Congress restricted the circumstances under which an insider—a user with authorized access—could be held liable for violating section 1030. "[I]nsiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage.

By contrast, outside intruders who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass." *See* S. Rep. No. 99-432, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479; *see also* S. Rep. No. 104-357, at 11 (1996), *available at* 1996 WL 492169.

According to this view, outsiders are intruders with no rights to use a protected computer system, and, therefore, they should be subject to a wider range of criminal prohibtions. Those who act without authorization can be convicted under any of the access offenses contained in the CFAA, which can be found in 18 U.S.C. § 1030(a)(1)-(5). However, users who exceed authorized access have at least some authority to access the computer system. Such users are therefore subject to criminal liability under more narrow circumstances. The offenses that can be charged based on exceeding authorized access are limited to those set forth in subsections (a)(1), (a)(2), and (a)(4). Table 2 below summarizes the authorization requirements of the CFAA offenses. If both the "without authorization" and "exceeds authorization" boxes are checked, the offense can be proven upon either showing. Note that subsections (a)(6) and (a)(7) are not access offenses and therefore have no authorization requirement.

Table 2. Authorized Access and Section 1030

§ 1030 Offense	Without Auth.	Exceeds Auth.	Not an element
(a)(1). Obtaining National Security Information	√	√	
(a)(2). Compromising Confidentiality	√	√	
(a)(3). Trespassing in a Govt. Computer	√		
(a)(4). Accessing to Defraud and Obtain Value	√	√	
(a)(5)(A)(i). Damaging Without Authorization			√
(a)(5)(A)(ii). Intentionally accessing and recklessly causing damage	√		
(a)(5)(A)(iii). Intentionally accessing and causing damage	√		
(a)(6). Trafficking in Passwords			√
(a)(7). Extortion Involving Threats to Damage a Computer			√

As Table 2 illustrates, the ability to charge certain conduct as a violation of the CFAA may turn upon whether or not a defendant can be shown to have acted without authorization, as opposed to having acted in excess of authorized access. The question of whether or not a given access was authorized has been the subject of frequent litigation in both criminal and civil cases under the CFAA. Cases interpreting the authorization elements of CFAA offenses have

generally followed the insider/outsider distinction, although not without some deviation. Traditional insider/outsider cases include *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), where an Internal Revenue Service employee was found to have exceeded his authorized access to IRS computer systems when he looked at taxpayer records for personal purposes, and *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001), where a Russian intruder broke into an American company's customer databases and was found to have acted without authorization.

While the universe of individuals who lack any authorization to access a computer is relatively easy to define, determining whether individuals who possess some legitimate authorization to access a computer have exceeded that authorized access may be more difficult. The term "exceeds authorized access" is defined as follows:

> [T]o access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

18 U.S.C. § 1030(e)(6).

The scope of any authorization hinges upon the facts of each case. In the simplest of prosecutions, a defendant without authorization to access a computer may intentionally bypass a technological barrier (such as password protection or system privileges) that prevented him from obtaining information on a computer network. However, many cases will involve exceeding authorized access, and establishing the scope of authorized access will be more complicated. The extent of authorization may turn upon the contents of an employment agreement or similar document, a terms of service notice, or a log-on banner outlining the permissible purposes for accessing a computer or computer network. *See Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435 (N.D. Tex. 2004) (user agreement); *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003) (various site notices); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000) (terms of use notice); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450-51 (E.D. Va. 1998) (terms of service agreement); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (employee confidentiality agreement).

In one case, however, an insider (a person with some limited authorization to use a system) strayed so far beyond the bounds of his authorization that the court treated him as having acted without authorization. *United States v.*

Morris, 928 F.2d 504 (2d Cir. 1991). Morris was convicted under a previous version of section 1030(a)(5), which punished "intentionally access[ing] a Federal interest computer without authorization." 18 U.S.C. § 1030(a)(5)(A) (1988). Morris created an Internet program known as a "worm," which spread to computers across the country and caused damage. To enable the worm to spread, Morris exploited vulnerabilities in two processes he was in fact authorized to use: "sendmail" (an email program) and "fingerd" (a program used to find out certain information about the users of other computers on the network). *Morris*, 928 F.2d. at 509-10.

On appeal, Morris argued that because he had authorization to engage in certain activities, such as sending electronic mail, on some university computers, he had merely exceeded authorized access, rather than having gained unauthorized access.

The Second Circuit rejected Morris' argument on three grounds. First, it held that the fact that the defendant had authorization to use certain computers on a network did not insulate his behavior when he gained access to other computers that were beyond his authorization. "Congress did not intend an individual's authorized access to one federal interest computer to protect him from prosecution, no matter what other federal interest computers he accesses." *Id.* at 511. Rather, "Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers." *Id.* at 510. Second, the court held that although Morris may have been authorized to use certain generally available functions—such as the email or user query services—on the systems victimized by the "worm," he misused that access in such a way to support a finding that his access was unauthorized. The court wrote that:

> Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.

Id.[1] Finally, the court held that even assuming the defendant's initial insertion of the worm simply exceeded his authorized access, evidence demonstrated

[1] Gauging whether an individual has exceeded authorized access based upon whether the defendant used the technological features of the computer system as "reasonably expected" was

that the worm was designed to spread to other computers and gain access to those computers without authorization by guessing their passwords.

"Authorized" is a fluid concept. Even when authorization exists, it can be withdrawn or it can lapse. In some instances, a court may invoke agency law to determine whether a defendant possessed or retained authorization to access a computer. *See, e.g., Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000) (finding that insiders with authorization to use a system can lose that authorization when they act as agents of an outside organization).

In *Shurgard*, employees were found to have acted "without authorization" when they accessed their employer's computers to appropriate trade secrets for the benefit of a competitor. The court applied principles of agency law, and concluded that the employees' authorized access to the employer's computers ended when they became agents of the competitor. *Id.* at 1124-25. *See International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (holding that an employee's access to data became unauthorized when breach of his duty of loyalty terminated his agency relationship). *See also Vi Chip Corp. v. Lee*, 438 F. Supp. 2d 1087, 1100 (N.D.Ca. 2006) (applying the holding of *Citrin* to an employee who deleted data after being informed that his employment was to be terminated). But see *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 at *5-7 (M.D. Fla. 2006) (criticizing *Citrin*).

Notably, *Shurgard*, *Citrin*, *Vi Chip*, and *Lockheed* all involved employees who were accused of abusing—e.g., selling, transferring, or destroying—data to which they had authorized access as part of their jobs. As a result, the plaintiffs were unable to establish that the defendants exceeded authorized access. Instead, in each of these cases the plaintiffs attempted to argue that access became unauthorized when the employee's purpose was not to benefit the employer. Essentially, each argued by reference to the Restatement (Second) of Agency that when the agent's duty of loyalty to his principal was breached, the relationship was terminated and subsequent access was unauthorized. *Shurgard,* 119 F. Supp. 2d at 1124-25; *Citrin*, 440 F.3d at 420-21; *Vi Chip,* 438 F. Supp. 2d. at 1100; *Lockheed*, 2006 WL 2683058 at *4. To prevail under this theory, a plaintiff needs to convince the court that the relationship was essentially

criticized by one court as too vague an approach. *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003) (in a civil case under § 1030(a)(4), involving whether use of a web scraper exceeded authorized access, rejected inferring "reasonable expectations" test in favor of express language on the part of the plaintiff).

terminated—i.e., the authorization to access the data was lost—even while the employee was still technically in its employ. The courts in *Shurgard*, *Citrin*, and *Vi Chip* agreed with this rationale, but the court in *Lockheed* did not. *Shurgard,* 119 F. Supp. 2d at 1124-25; *Citrin*, 440 F.3d at 420-21; *Vi Chip,* 438 F. Supp. 2d. at 1100; *Lockheed*, 2006 WL 2683058 at *5-7. Prosecutors faced with similar facts may want to consider charging an offense that does not contain an authorization requirement, such as section 1030(a)(5)(A)(i).

One court found that insiders acted without authorization when they violated clearly defined computer access policies. *See, e.g., America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (holding that AOL members acted without authorization when they used AOL network to send unsolicited bulk emails in violation of AOL's member agreement). *But see America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255 (N.D. Iowa 2000) (noting that no other published decision contains the same interpretation as *America Online, Inc. v. LCGM, Inc.* on the issue of unauthorized access).

Typically, however, persons who are employees or licensees of the entity whose computer they used are held liable for exceeding authorized access as opposed to unauthorized access. *See EF Cultural Travel*, 274 F.3d at 582-84 (holding that a former employee who violated a confidentiality agreement by providing information about accessing a protected computer system could be liable for exceeding authorized access). In *SecureInfo Corp. v. Telos Corp.,* 387 F. Supp. 2d 593 (E.D. Va. 2005), the Court dismissed a claim that defendants, who gained access to a protected computer due to breach of a software license by a licensee, either exceeded authorized access or gained unauthorized access. The court believed that the licensee had given the defendants authority to use the computer system, which undercut the plaintiff's unauthorized use claim. *Id.* at 608-09. Moreover, since it was the licensee and not the defendants who agreed to the terms of the license, the defendants were not bound to the use limitations, and therefore, had not exceeded authorized access. *Id.* at 609-10. The court noted, however, that had the licensee—as opposed to the persons who gained access to the system via the licensee—been sued for exceeding authorized use, they may have been found liable under theory set forth in *EF Cultural Travel. Id.* at 609 (*citing EF Cultural Travel BV*, 274 F.3d at 582).

The *SecureInfo* decision is troublesome in that it could arguably be read to support the proposition that users who are granted access to a system by an authorized user cannot be found liable under either an unauthorized use

or an in excess of authorization theory. Presumably, however, had the third parties used their authorized access to obtain information unavailable to even licensed users, the court would have held them liable. The better reading of this decision is that courts may be reluctant to predicate civil liability, much less criminal liability, under the CFAA solely upon a violation of a software licensing agreement.

In sum, "without authorization" generally refers to intrusions by outsiders, but some courts have also applied the term to intrusions by insiders who access computers other than the computer they are authorized to use, intrusions by insiders acting as agents for outsiders, and intrusions by insiders who violate clearly defined access policies. Section 1030 imposes greater liability on outsiders because their very presence on the computer or network constitutes trespass. Thus, certain subsections (18 U.S.C. §§ 1030(a)(3), (a)(5)(A)(ii), & (a)(5)(A)(iii)) criminalize actions based upon access without authorization, but do not impose the same liability if the access merely exceeds authorization. In any event, it is clear that courts treat the issue of authority to access as a question of fact under the specific circumstances of each case. Prosecutors should consider not only whether the access breached technical security measures (such as passwords), but also employer policies, banners, user agreements, contracts, licenses, or similar items.

B. Obtaining National Security Information: 18 U.S.C. § 1030(a)(1)

The infrequently-used section 1030(a)(1) punishes the act of obtaining national security information without or in excess of authorization and then willfully providing or attempting to provide the information to an unauthorized recipient, or willfully retaining the information.

Any steps in investigating or indicting a case under section 1030 (a)(1) require the prior approval of the National Security Division of the Department of Justice, through the Counterespionage Section. See USAM 9-90.020. Please contact them at (202) 514-1187.

Summary

1. Knowingly access computer without or in excess of authorization
2. obtain national security information
3. reason to believe the information could injure the U.S. or benefit a foreign nation
4. willful communication, delivery, transmission (or attempts)
   OR
   willful retention of the information

Title 18, United States Code, Section 1030(a)(1) provides:

Whoever–

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it …

shall be punished as provided in subsection (c) of this section.

1. Knowingly Access a Computer Without or In Excess of Authorization

A violation of this section requires proof that the defendant knowingly accessed a computer without authorization or in excess of authorization. This covers both completely unauthorized individuals who intrude into a computer containing national security information as well as insiders with limited privileges who manage to access portions of a computer or computer network to which they have not been granted access. The scope of authorization will depend upon the facts of each case. However, it is worth noting that computers and computer networks containing national security information will normally be classified and incorporate security safeguards and access controls of their own, which should facilitate proving this element.

Please see page 4 for the discussion of the concept of access without or in excess of authorization.

2. Obtain National Security Information

A violation of this section requires that the information obtained is national security information, meaning information "that has been determined

by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954." An example of national security information used in section 1030(a)(1) would be classified information obtained from a Department of Defense computer or restricted data obtained from a Department of Energy computer.

3. Information Could Injure the United States or Benefit a Foreign Nation

A violation of this section requires proof that the defendant had reason to believe that the national security information so obtained could be used to the injury of the United States or to the advantage of any foreign nation. The fact that the national security information is classified or restricted, along with proof of the defendant's knowledge of that fact, should be sufficient to establish this element of the offense.

4. Willful Communication, Delivery, Transmission, or Retention

A violation of this section requires proof that the defendant willfully communicated, delivered, or transmitted the national security information, attempted to do so, or willfully retained the information instead of delivering it to the intended recipient. This element could be proven through evidence showing that the defendant did any of the following: (a) communicated, delivered, or transmitted national security information, or caused it to be communicated, delivered, or transmitted, to any person not entitled to receive it; (b) attempted to communicate, deliver, or transmit national security information, or attempted to cause it to be communicated, delivered, or transmitted to any person not entitled to receive it; or (c) willfully retained national security information and failed to deliver it to an officer or employee of the United States who is entitled to receive it in the course of their official duties.

5. Penalties

Convictions under this section are felonies punishable by a fine, imprisonment for not more than ten years, or both. 18 U.S.C. § 1030(c)(1)(A). A violation that occurs after another conviction under section 1030 is punishable by a fine, imprisonment for not more than twenty years, or both. 18 U.S.C. § 1030(c)(1)(B).

6. Historical Notes

Section 1030(a)(1) was originally enacted in 1984 and was substantially amended in 1996. As originally enacted, section 1030(a)(1) provided that anyone who knowingly accessed a computer without authorization or in excess of authorization and obtained classified information "with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation" was subject to a fine or imprisonment for not more than ten years for a first offense. This scienter element mirrored that of 18 U.S.C. § 794(a), the statute that prohibits gathering or delivering defense information to aid a foreign government. Section 794(a), however, provides for life imprisonment, whereas section 1030(a)(1) is only a ten-year felony. Based on that distinction, Congress amended section 1030(a)(1) in 1996 to track more closely the language of 18 U.S.C. § 793(e), which also provides a maximum penalty of ten years' imprisonment, for obtaining from any source certain information connected with the national defense and thereafter communicating or attempting to communicate it in an unauthorized manner.

Violations of this subsection are charged quite rarely. The reason for this lack of prosecution may well be the close similarities between sections 1030(a)(1) and 793(e). In situations where both statutes are applicable, prosecutors may tend towards using section 793(e), for which guidance and precedent are more prevalent.

However, a four-count information was filed in the U.S. District Court for the District of New Jersey on May 4, 2006, which charged Leandro Aragoncillo, an FBI intelligence analyst assigned to the Ft. Monmouth Information Technology Center, with, among other things, a section 1030(a)(1) violation. Aragoncillo pleaded guilty to the information, and admitted that he used his FBI computer to access classified documents through the FBI's Automated Case System and transmit the information contained in the documents to former and current officials of the Philippine government. For more information about this case, please contact the Counterespionage Section of the National Security Division.

Although sections 793(e) and 1030(a)(1) overlap, the two statutes do not reach exactly the same conduct. Section 1030(a)(1) requires proof that the individual knowingly accessed a computer without or in excess of authority and thereby obtained national security information, and subsequently

performed some unauthorized communication or other improper act with that data. In this way, it focuses not only on the possession of, control over, or subsequent transmission of the information (as section 793(e) does), but also focuses on the improper use of a computer to obtain the information itself. Existing espionage laws such as section 793(e) provide solid grounds for the prosecution of individuals who attempt to peddle governmental secrets to foreign governments. However, when a person, without authorization or in excess of authorized access, deliberately accesses a computer, obtains national security information, and seeks to transmit or communicate that information to any prohibited person, prosecutors should consider charging a violation section 1030(a)(1) in addition to considering charging a violation of Section 793(e).

One other issue to note is that section 808 of the USA PATRIOT Act added section 1030(a)(1) to the list of crimes in that are considered to be "Federal Crime[s] of Terrorism" under 18 U.S.C. § 2332b(g)(5)(B). This addition affects prosecutions under section 1030(a)(1) in three ways. First, because offenses listed under section 2332b(g)(5)(B) are now incorporated into 18 U.S.C. § 3286, the statute of limitation for subsection (a)(1) is extended to eight years, and is eliminated for offenses that resulted in, or created a foreseeable risk of, death or serious bodily injury to another person. Second, the term of supervised release after imprisonment for any offense listed under section 2332b(g)(5)(B) that resulted in, or created a foreseeable risk of, death or serious bodily injury to another person, can be any term of years or life. 18 U.S.C. § 3583. Formerly, the maximum term of supervised release for any violation of section 1030 was five years. Third, the USA PATRIOT Act added the offenses listed in section 2332b(g)(5)(B) to 18 U.S.C. § 1961(1), making them predicate offenses for prosecution under the Racketeer Influenced and Corrupt Organizations (RICO) statute. As a result, any "RICO enterprise" (which may include terrorist groups) that carries out acts of cyberterrorism in violation of section 1030(a)(1) (or section 1030(a)(5)(A)(i)) can now be prosecuted under the RICO statute.

C. Compromising Confidentiality: 18 U.S.C. § 1030(a)(2)

Summary

1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information from:
   - financial records of financial institution or consumer reporting agency
     OR
   - the U.S. government
     OR
   - a protected computer if interstate or foreign communication involved

The distinct but overlapping crimes established by the three subsections of section 1030(a)(2) punish the unauthorized access of different types of information and computers. Violations of this section are misdemeanors unless aggravating factors exist. Also, some intrusions may violate more than one subsection. For example, a computer intrusion into a federal agency's computer might be covered under the latter two subsections.

Section 1030(a)(2) does not impose a monetary threshold for a violation, in recognition of the fact that some invasions of privacy do not lend themselves to monetary valuation but still warrant federal protection. If not authorized, downloading sensitive personnel information from a company's computer (via an interstate communication) or gathering personal data from the National Crime Information Center would both be serious violations of privacy which do not easily lend themselves to a dollar valuation of the damage. Although there is no monetary threshold for establishing an offense under section 1030(a)(2), the value of the information obtained during an intrusion is important when determining whether a violation constitutes a misdemeanor or a felony.

Title 18, United States Code, Section 1030(a)(2) provides:

Whoever–

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains–

> *(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);*
>
> *(B) information from any department or agency of the United States; or*

(C) information from any protected computer if the conduct involved an interstate or foreign communication ...

shall be punished as provided in subsection (c) of this section.

1. Intentionally Access a Computer

A violation of this section requires that the defendant actually be the one to access a computer without authorization rather than merely receive information that was accessed without authorization by another. For example, if A obtains information in violation of section 1030(a)(2) and forwards it to B, B has not violated this section, even if B knew the source of the information. *See Role Models America, Inc. v. Jones*, 305 F. Supp. 2d 564 (D. Md. 2004). Of course, B might be subject to prosecution for participating in a criminal conspiracy to violate this section.

2. Without or In Excess of Authorization

Please see page 4 for the discussion of access without or in excess of authorization.

3. Obtained Information

The term "obtaining information" is an expansive one which includes merely viewing information online without downloading or copying it. *See* S. Rep. No. 99-432, at 6; *America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255 (N.D. Iowa 2000). Information stored electronically can be obtained not only by actual physical theft, but by "mere observation of the data." *Id*. The "crux of the offense under subsection 1030(a)(2)(C) ... is the abuse of a computer to obtain the information." *Id*.

"Information" includes intangible goods, settling an issue raised by the Tenth Circuit's decision in *United States v. Brown*, 925 F.2d 1301, 1308 (10th Cir. 1991). In *Brown*, the appellate court held that purely intangible intellectual property, such as a computer program, did not constitute goods or services that can be stolen or converted. In the 1996 amendments to section 1030, Congress clarified this issue, stating that section 1030(a)(2) would "ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected." S. Rep. No. 104-357, at 7, *available at* 1996 WL 492169.

4. Financial Institution or Consumer Reporting Agency

To prove a violation of section 1030(a)(2)(A), obtaining information related to the Fair Credit Reporting Act (FCRA), the violation must be willful. *See Ausherman v. Bank of America Corp.*, 352 F.3d 896 at 900 n.4 (4th Cir. 2003). To prove willfulness under the FCRA, the government must show that the defendant knowingly and intentionally committed an act in conscious disregard for the rights of a consumer. *Id*.

5. Department or Agency of the United States

Whether a company working as a private contractor for the government constitutes a "department or agency of the United States" for purposes of prosecution under subsection (a)(2)(B) has not been addressed by any court. However, the argument that private contractors are intended to be covered by this section may be undercut by section 1030(a)(3), which includes language permitting prosecution of trespass into government systems *and* non-government systems, if "such conduct affects that use by or for the Government of the United States." The existence of this language suggests that if Congress had intended to extend the reach of section 1030(a)(2) beyond computers owned by the federal government, it would have done so using language it used elsewhere in section 1030.

6. Protected Computer

The term "protected computer" is defined in section 1030(e)(2) and is discussed in the "Key Definitions" discussion on page 3.

Note that a violation of this subsection must involve an actual interstate or foreign communication and not merely the use of an interstate communication mechanism, as other parts of the CFAA allow. The intent of this subsection is to protect against the interstate or foreign theft of information by computer, not to give federal jurisdiction over all circumstances in which someone unlawfully obtains information via a computer. *See* S. Rep. No 104-357. Therefore, using the Internet or connecting by telephone to a network may not be sufficient to charge a violation of this subsection where there is no evidence that the victim computer was accessed using some type of interstate or foreign communication.

7. Penalties

Violations of section 1030(a)(2) are misdemeanors punishable by a fine or a one-year prison term, unless aggravating factors apply. 18 U.S.C. § 1030(c)(2)(A). Merely obtaining information worth less than $5,000 is a misdemeanor, unless committed after a conviction of another offense under section 1030. 18 U.S.C. § 1030(c)(2)(C). A violation or attempted violation of section 1030(a)(2) is a felony if:

- committed for commercial advantage or private financial gain,
- committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or
- the value of the information obtained exceeds $5,000.

18 U.S.C. § 1030(c)(2)(B). If the aggravating factors apply, a violation is punishable by a fine, up to five years' imprisonment, or both.

Any reasonable method can be used to establish the value of the information obtained. For example, the research, development, and manufacturing costs or the value of the property "in the thieves' market" can be used to meet the $5,000 valuation. *See, e.g., United States v. Stegora*, 849 F.2d 291, 292 (8th Cir. 1988). The terms "for purposes of commercial advantage or private financial gain" and "for the purpose of committing any criminal or tortious act" are taken from copyright law (17 U.S.C. § 506(a)) and the wiretap statute (18 U.S.C. § 2511(2)(d)), respectively.

8. Historical Notes

Originally, section 1030(a)(2) protected individual privacy by criminalizing unauthorized access to computerized information and credit records relating to customers' relationships with financial institutions. *See* S. Rep. No. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483; *see also* S. Rep. 104-357, at 7; *America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1275 (N.D. Iowa 2000). In 1996, Congress expanded the scope of the section by adding two subsections that also protected information on government computers (§ 1030(a)(2)(B)) and computers used in interstate or foreign communication (§ 1030(a)(2)(C)).

In 1986, Congress changed the scienter requirement from "knowingly" to "intentionally." *See* Pub. L. No. 99-474, § 2(a)(1). The first reason for the change was to ensure that only intentional acts of unauthorized access were prohibited, rather than "mistaken, inadvertent, or careless" acts of unauthorized access. S.

Rep. No. 99-432, at 5, 1986 U.S.C.C.A.N. at 2483. The second reason for the change was a concern that the "knowingly" standard "might be inappropriate for cases involving computer technology." *Id.* The specific concern was that a scienter requirement of "knowingly" might include an individual "who inadvertently 'stumble[d] into' someone else's computer file or computer data," especially where such individual was authorized to use a particular computer. *Id.* at 6, 1986 U.S.C.C.A.N. at 2483. The Senate Report offered that "[t]he substitution of an 'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." *Id.*, 1986 U.S.C.C.A.N. at 2484.

Section 1030(a)(2) applies to computer access "without authorization" and access that "exceeds authorized access." The intent of this distinction is to differentiate between the conduct of insiders (i.e., individuals who have been granted some authority to access a computer) and outsiders (i.e., individuals who have no authority to access a computer). *See* S. Rep. No. 99-432, at 10, 1986 U.S.C.C.A.N. at 2479; *see also* S. Rep. No. 104-357, The National Information Infrastructure Protection Act of 1996, at 10-11 (1996).

D. Trespassing in a Government Computer: 18 U.S.C. § 1030(a)(3)

Summary

1. Intentionally access
2. without authorization
3. a nonpublic computer of the U.S. that was exclusively for the use of the U.S. or was used by or for the U.S.
4. affected U.S. use of computer

Section 1030(a)(3) protects against "trespasses" by outsiders into federal government computers, even when no information is obtained during such trespasses. Congress limited this section's application to outsiders out of concern that federal employees could become unwittingly subject to prosecution or punished criminally when administrative sanctions were more appropriate. S. Rep. No. 99-432, at 7, 1986 U.S.C.C.A.N. at 2485. However, Congress intended interdepartmental trespasses (rather than intradepartmental trespasses) to be punishable under section 1030(a)(3). *Id.*

Note that section 1030(a)(2) applies to many of the same cases in which section 1030(a)(3) could be charged. In such cases, section 1030(a)(2) may be the preferred charge because a first offense of section 1030(a)(2) may be

charged as a felony if certain aggravating factors are present, while a first offence of section 1030(a)(3) is only a misdemeanor.

Title 18, United State Code, Section 1030(a)(3) provides:

Whoever–

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States ….

shall be punished as provided in subsection (c) of this section.

1. Intentionally Access

The meaning of this term under this section is identical to the meaning under section 1030(a)(2), discussed on page 16.

2. Without Authorization

By requiring that the defendant act without authorization to the computer and not criminalizing merely exceeding authorized access to a computer, section 1030(a)(3) does not apply to situations in which employees merely "'exceed authorized access" to computers in their own department. S. Rep. No. 99-432. However, Congress also offered that section 1030(a)(3) applies "where the offender's act of trespass is interdepartmental in nature." *Id.* at 8. Thus, while federal employees may not be subject to prosecution under section 1030(a)(3) as insiders as to their own agency's computers, they may be eligible for prosecution as outsiders in regard to intrusions into other agencies' computers.

Please see page 4 for the discussion of the concept of access without or in excess of authorization.

3. Nonpublic Computer of the United States

"Nonpublic" includes most government computers, but not Internet servers that, by design, offer services to members of the general public. For example, a government agency's database server is probably nonpublic, while the same agency's web servers and domain name servers are "public."

The computer must be "of"—meaning owned or controlled by—a department or agency of the United States.

The computer must also be either exclusively for the use of the United States, or at least used "by or for" the Government of the United States in some capacity. For example, if the United States has obtained an account on a private company's server, that server is used "by" the United States even though it is not owned by the United States.

4. Affected United States' Use of Computer

Demonstrating that the attacked computer is affected by an intrusion should be simple. Almost any network intrusion will affect the government's use of its computers because any intrusion potentially affects the confidentiality and integrity of the government's network and often requires substantial measures to reconstitute the network.

Section 1030(a)(3) "defines as a criminal violation the knowing unauthorized access or use of the system for any unauthorized purpose." *Sawyer v. Department of Air Force,* 31 M.S.P.R. 193, 196 (M.S.P.B. 1986). Notably, it is *not* necessary to demonstrate that the intruder obtained any information from the computer, or that the intruder's trespass damaged the computer. It is not even necessary to show that the intruder's conduct "adversely" affected the government's operation of a computer. Under § 1030(a)(3), there are no benign intrusions into government computers.

5. Statutory Penalties

Violations of this subsection are punishable by a fine and up to one year in prison, 18 U.S.C. § 1030(c)(2)(A), unless the individual has previously been convicted of a section 1030 offense, in which case the punishment increases to a maximum of ten years in prison, 18 U.S.C. § 1030(c)(2)(c).

6. Relation to Other Statutes

Section 1030(a)(3) is not charged often, and few cases interpret it. This lack is probably because section 1030(a)(2) applies in many of the same cases in which section 1030(a)(3) could be charged. In such cases, section 1030(a)(2) may be the preferred charge because statutory sentencing enhancements sometimes allow section 1030(a)(2) to be charged as a felony on the first offense. A violation of section 1030(a)(3), on the other hand, is only a misdemeanor for a first offense.

7. Historical Notes

Congress added the term "nonpublic" in 1996, in recognition of the occasions when a department or agency authorizes access to some portions of its systems by the public, such as websites and interactive services. This addition eliminated the potential defense that intruders were not "without authorization to access *any* computer," if they had been given authority to access websites and other public networked services offered by the government. By adding the word "nonpublic," Congress clarified that persons who have no authority to access nonpublic computers of a department or agency may be convicted under section 1030(a)(3), even if they are allowed to access publicly available computers.

During enactment of section 1030(a)(3), the Department of Justice expressed concern that the section could be interpreted to require that the offender's conduct harm the overall operation of the Government, which would be an exceedingly difficult showing for federal prosecutors. Congress responded in 1996 by drafting section 1030(a)(3) so that an offender's conduct need only affect the use of the Government's operation of the attacked computer rather than affect the Government as a whole. *See* S. Rep. No. 99-432.

E. Accessing to Defraud and Obtain Value: 18 U.S.C. § 1030(a)(4)

Summary

1. Knowingly access a protected computer without or in excess of authorization
2. with intent to defraud
3. the access furthered the intended fraud
4. obtained anything of value, including use if value exceeded $5000

When deciding how to charge a computer hacking case, prosecutors should consider this section as an alternative to section 1030(a)(2) where evidence of fraud exists, particularly because this section is a felony whereas subsection (a)(2) is a misdemeanor (unless certain aggravating factors apply).

Prosecutors may also want to consider charges under the wire fraud statute, 18 U.S.C. § 1343, which requires proof of many elements similar to those needed for section 1030(a)(4), but carries stiffer penalties. For more

detail on the comparison, please see page 29. For more discussion about wire fraud, please see page 90.

Title 18, United State Code, Section 1030(a)(4) provides:

Whoever–

(4) 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 …

shall be punished as provided in subsection (c) of this section.

1. Knowingly Access Without or In Excess of Authorization

Please see page 4 for the discussion of the concept of access without or in excess of authorization.

2. With Intent to Defraud

The phrase "knowingly and with intent to defraud" is not defined by section 1030. Very little case law under section 1030 exists as to its meaning, leaving open the question of how broadly a court will interpret the phrase. On one hand, courts might interpret "intent to defraud" as requiring proof of the elements of common law fraud.[2] On the other hand, courts might give more liberal meaning to the phrase "intent to defraud" and allow proof of mere wrongdoing or dishonesty to suffice.

In examining the phrase "to defraud" in the mail and wire fraud statutes,[3] the Supreme Court rejected the notion that every "scheme or artifice that in its necessary consequence is one which is calculated to injure another [or] to deprive him of his property wrongfully" constitutes fraud under the mail fraud provision. *Fasulo v. United States*, 272 U.S. 620, 629 (1926). In *Fasulo*, the court stated that "broad as are the words 'to defraud,' they do not include threat

[2] The elements of common law fraud are: "(1) a false representation (2) in reference to a material fact (3) made with knowledge of its falsity (4) and with intent to deceive (5) with action taken in reliance upon the representation." *United States v. Kiefer*, 228 F.2d 448 (D.C. Cir. 1955).

[3] Identical standards apply to the "scheme to defraud" under both the mail and the wire fraud statutes. *See United States v. Antico*, 275 F.3d 245 (3d Cir. 2001).

and coercion through fear or force." *Id.* at 628. Instead, the Supreme Court placed emphasis on the central role of *deception* to the concept of fraud—"the words 'to defraud' ... primarily mean to cheat, ... usually signify the deprivation of something of value by trick, deceit, chicane, or overreaching, and ... do not extend to theft by violence, or to robbery or burglary." *Id.* at 627 (construing *Hammerschmidt v. United States*, 265 U.S. 182 (1924)).

A broader alternative definition can be found in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000), a civil case involving section 1030(a)(4). In that case, the court favored an expansive interpretation of "intent to defraud." In denying the defendant's motion to dismiss, the court held that the word "fraud" as used in section 1030(a)(4) simply means "wrongdoing" and does not require proof of the common law elements of fraud. *Id.* at 1126 (construing *United States v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997)). Thus, the plaintiff stated a sufficient cause of action under section 1030(a)(4) by alleging that the defendant participated in "dishonest methods to obtain the plaintiff's secret information." *Id.*

Shurgard does not directly address the Supreme Court decision in *Fasulo*, but nevertheless provides some basis for interpreting "fraud" in its broadest sense (i.e., finding "fraud" when there is evidence of "wrongdoing," as opposed to requiring proof of "trick, deceit, chicane, or overreaching"). *Cf.* 132 Cong. Rec. S4072-02, 99th Cong., 2d. Sess. (1986) ("The acts of 'fraud' that we are addressing in proposed § 1030(a)(4) are essentially thefts in which someone uses a [protected computer] to wrongly obtain something of value from another").

In discussing the creation of section 1030(a)(4), Congress specifically noted that "[t]he scienter requirement for this subsection, 'knowingly and with intent to defraud,' is the same as the standard used for 18 U.S.C. 1029 relating to credit card fraud." *See* S. Rep. No. 99-432, at 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488. Interestingly, despite having specifically discussed the mail and wire fraud statutes in the context of section 1030(a)(4), the Committee did not relate the scienter requirement of the term "to defraud" to the use of the term in the mail and wire fraud statutes, leaving open the question of whether the meaning and proof of "to defraud" is the same for sections 1030(a)(4) and 1029, as it is for the mail and wire fraud statutes. As it is, there are no reported cases discussing the meaning of "to defraud" under section 1029.

3. Access Furthered the Intended Fraud

The defendant's illegal access of the protected computer must "further" a fraud. Accessing a computer without authorization—or, more often, exceeding authorized access—can further a fraud in several ways. For example:

- This element is met if a defendant alters or deletes records on a computer, and then receives something of value from an individual who relied on the accuracy of those altered or deleted records. In *United States v. Butler,* 16 Fed. Appx. 99 (4th Cir. 2001) (unpublished disposition), the defendant altered a credit reporting agency's records to improve the credit ratings of his coconspirators, who then used their improved credit rating to make purchases. In *United States v. Sadolsky,* 234 F.3d 938 (6th Cir. 2000), the defendant used his employer's computer to credit amounts for returned merchandise to his personal credit card.
- This element is met if a defendant obtains information from a computer, and then later uses that information to commit fraud. For example, in *United States v. Lindsley,* 2001 WL 502832 (5th Cir. 2001) (unpublished), the defendant accessed a telephone company's computer without authorization, obtained calling card numbers, and then used those calling card numbers to make free long-distance telephone calls.
- This element is met if a defendant uses a computer to produce falsified documents which are later used to defraud. For example, in *United States v. Bae,* 250 F.3d 774 (D.C. Cir. 2001), the defendant used a lottery terminal to produce back-dated tickets with winning numbers, and then turned those tickets in to collect lottery prizes.

The term "by means of such conduct" explicitly links the unauthorized accessing of a protected computer to the furthering of the intended fraud. In creating this link, Congress wished to distinguish those cases of computer trespass where the trespass is used to further the fraud (covered by § 1030(a)(4)) from those cases of fraud that involve a computer but the computer is only tangential to the crime (not covered by § 1030(a)(4)). *See* S. Rep. No. 99-432, at 9, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487.

In order to fall within section 1030(a)(4), "the use of the computer must be more directly linked to the intended fraud." The section does not apply simply because "the offender signed onto a computer at some point near to the commission or execution of the fraud." *Id.* More explicitly, a fraudulent

scheme does not constitute computer fraud just because a computer was used "to keep records or to add up [the] potential 'take' from the crime." *Id.*

4. Obtains Anything of Value

This element is easily met if the defendant obtained money, cash, or a good or service with measurable value. Two more difficult cases arise when the defendant obtains only the use of a computer and when the defendant obtains only information.

Use of the computer as a thing of value

The statute recognizes that the use of a computer can constitute a thing of value, but this element is satisfied only if the value of such use is greater than $5,000 in any one-year period.

This condition will be met only in rare cases. At the time the statute was written, it was common for owners of top-of-the-line supercomputers to rent the right to run programs on their computer by the hour. In 1986, for example, an hour of time on a Cray X-MP/48 supercomputer reportedly cost $1,000. William F. Eddy, *Rejoinder,* Statistical Science, Nov. 1986, 451, 453. Conceivably, repeated and sustained use of a very expensive modern computer could reach the statutory threshold within one year.

Data or information as a thing of value

Aside from the "computer use" exception, subsection (a)(4) has no minimum dollar amount, unlike subsection (a)(5). Still, the legislative history suggests that some computer data or information, alone, is not valuable enough to qualify. *See* S. Rep. 99-432, at 9, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487) ("In intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass."). In other words, if all that is obtained are the results of port scans, or the names and IP addresses of other servers, it may not count as something of value.

One case of particular note in this area is *United States v. Czubinski,* 106 F.3d 1069 (1st Cir. 1997). While the *Czubinski* case turned on the specific facts, the court's discussion can be instructive in assessing the parameters of the term "something of value." Specifically, *Czubinski* was employed as a Contact Representative in the Boston office of the Taxpayer Services Division

of the Internal Revenue Service (IRS). As part of his official duties, Czubinski routinely accessed taxpayer-related information from an IRS computer system using a valid password provided to Contact Representatives. Despite IRS rules plainly forbidding employees from accessing taxpayer files outside the course of their official duties, Czubinski carried out numerous unauthorized searches of taxpayer records on a number of occasions. Based upon these actions, he was indicted and convicted for wire fraud and computer fraud.

On appeal, Czubinski argued that his conviction for violating section 1030(a)(4) should be overturned because he did not obtain "anything of value." In reviewing the facts surrounding Czubinski's actions, the First Circuit agreed with Czubinski, stating that "[t]he value of information is relative to one's needs and objectives; here, the government had to show that the information was valuable to Czubinski in light of a fraudulent scheme. The government failed, however, to prove that Czubinski intended anything more than to satisfy idle curiosity." *Id.* at 1078.

Further elaborating on its holding, the court went on to explain that:

> [t]he plain language of section 1030(a)(4) emphasizes that more than mere unauthorized use is required: the 'thing obtained' may not merely be the unauthorized use. It is the showing of some additional end—to which the unauthorized access is a means—that is lacking here. The evidence did not show that Czubinski's end was anything more than to satisfy his curiosity by viewing information about friends, acquaintances, and political rivals. No evidence suggests that he printed out, recorded, or used the information he browsed. No rational jury could conclude beyond a reasonable doubt that Czubinski intended to use or disclose that information, and merely viewing information cannot be deemed the same as obtaining something of value for the purposes of this statute.

Id.[4]

[4] *Czubinski* has been incorrectly cited for the proposition that it is not enough to temporarily download information just long enough to view it on a computer display to satisfy the "of value" prong of § 1030(a)(4). *See United States v. Ivanov,* 175 F. Supp. 2d 367, 371 (D. Conn. 2001) ("In order for Ivanov to violate § 1030(a)(4), it was necessary that he do more than merely access OIB's computers and view the data.") (*citing Czubinski*, 106 F.3d at 1078). A careful reading of *Czubinski*, however, illustrates that the court's discussion of printing out or downloading information was meant only as an example of how the government might have proven that Czubinski had accessed the information to further his fraud and thereby obtain

The parameters of what constitutes a "thing of value" were further explored in *In re America Online, Inc.*, 168 F. Supp. 2d 1359 (S.D. Fla. 2001). Specifically, America Online (SSOL) was sued by computer users and competitor Internet service providers, alleging that AOL's software had caused damage to users' computers and had blocked utilization of competitors' software by potential users. *Id.* In moving to dismiss the section 1030(a)(4) allegation, AOL argued that the plaintiffs could not make out an actionable claim because they had failed to plead that AOL had deprived them of "anything of value." *Id.* at 1379. In response, the plaintiffs asserted that AOL's actions had deprived them of their subscribers "custom and trade" and that this interest constituted a "thing of value." *Id.*

In distinguishing the case from *Czubinski*, the *America Online* court noted that "AOL allegedly has been motivated by more than the mere satisfaction of its curiosity [as was allegedly the sole motivation of the defendant in *Czubinski*]. AOL's alleged end is to obtain a monopoly, or at least secure its stronghold, as an ISP." *America Online*, at 1379-80. Noting that the "typical item of value" in cases brought under the CFAA is usually data, the court observed that "in other areas of the law, customers have been found to be a thing of value." *Id.* at 1380. The court therefore found that "damage to an ISP's goodwill and reputation is actionable under the CFAA" and that "[b]ecause [the plaintiff] has alleged that AOL's actions have interfered with its relationships with its existing customers and potential subscribers, it has alleged that AOL has obtained something of value within the meaning of 18 U.S.C. § 1030(a)(4)." *Id.*

5. Statutory Penalties

A violation of section 1030(a)(4) is punishable by a fine and up to five years in prison, unless the individual has been previously convicted of a section 1030 offense, in which case the punishment increases to a maximum of ten years in prison. 18 U.S.C. § 1030(c)(3).

---

something of value; in other words, that his accessing of information was not done merely to satisfy his idle curiosity. Indeed, if a defendant were to access and view information from a protected computer, without or in excess of authorization, and then use that information to engage in identity theft, that defendant could likely be prosecuted for violating § 1030(a)(4) even if the defendant merely memorized the information and never downloaded or printed it out. This reading would likewise be consistent with the interpretation of the word "obtains" in the context of § 1030(a)(2) violations, which does not require copying or "asportation." Please see page 16 for the discussion of "Obtained Information" under § 1030(a)(2).

6. Relation to Other Statutes

In appropriate cases, prosecutors may also want to consider charges under the wire fraud statute, 18 U.S.C. § 1343, which requires proof of many elements similar to those needed for section 1030(a)(4). Unlike section 1030(a)(4), however, which is punishable by a maximum of 5 years in prison (assuming the defendant does not have other prior § 1030 convictions), wire fraud carries stiffer penalties and is punishable by a maximum of 20 years in prison, or 30 years if the violation affected a financial institution. *Compare* 18 U.S.C. § 1030(a)(3) *with* 18 U.S.C. § 1343.

7. Historical Notes

Although section 1030(a)(4) bears similarities to the federal mail fraud statute (18 U.S.C. § 1341) and wire fraud statute (18 U.S.C. § 1343), section 1030(a)(4) does not have the same broad jurisdictional sweep as the mail and wire fraud statutes. *See* S. Rep. No. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487 ("It has been suggested that the Committee approach all computer fraud in a manner that directly tracks the existing mail fraud and wire fraud statutes. However, the Committee was concerned that such an approach might permit prosecution under this subsection of acts that do not deserve classification as 'computer fraud'."). The specific concern expressed was "that computer usage that is wholly extraneous to an intended fraud might nevertheless be covered by this subsection if the subsection were patterned directly after the current mail fraud and wire fraud laws." *Id.*

F. Damaging a Computer or Information: 18 U.S.C. § 1030(a)(5)

Criminals can cause harm to computers in a wide variety of ways. For example, an intruder who gains unauthorized access to a computer can send commands that delete files or shut the computer down. Alternatively, intruders can initiate a "denial of service attack" that floods the victim computer with useless information and prevents legitimate users from accessing it. In a similar way, a virus or worm can use up all of the available communications bandwidth on a corporate network, making it unavailable to employees. In addition, when a virus or worm penetrates a computer's security, it can delete files, crash the computer, install malicious software, or do other things that impair the

computer's integrity. Prosecutors can use section 1030(a)(5) to charge all of these different kinds of acts.

Section 1030(a)(5) criminalizes a variety of actions that cause computer systems to fail to operate as their owners would like them to operate. Damaging a computer can have far-reaching effects. For example, a business may not be able to operate if its computer system stops functioning or it may lose sales if it cannot retrieve the data in a database containing customer information. Similarly, if a computer that operates the phone system used by police and fire fighters stops functioning, people could be injured or die as a result of not receiving emergency services. Such damage to a computer can occur following a successful intrusion, but it may also occur in ways that do not involve the unauthorized access of a computer system.

Title 18, United State Code, Section 1030(a)(5) provides:

Whoever–

(5)(A)(i) 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;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

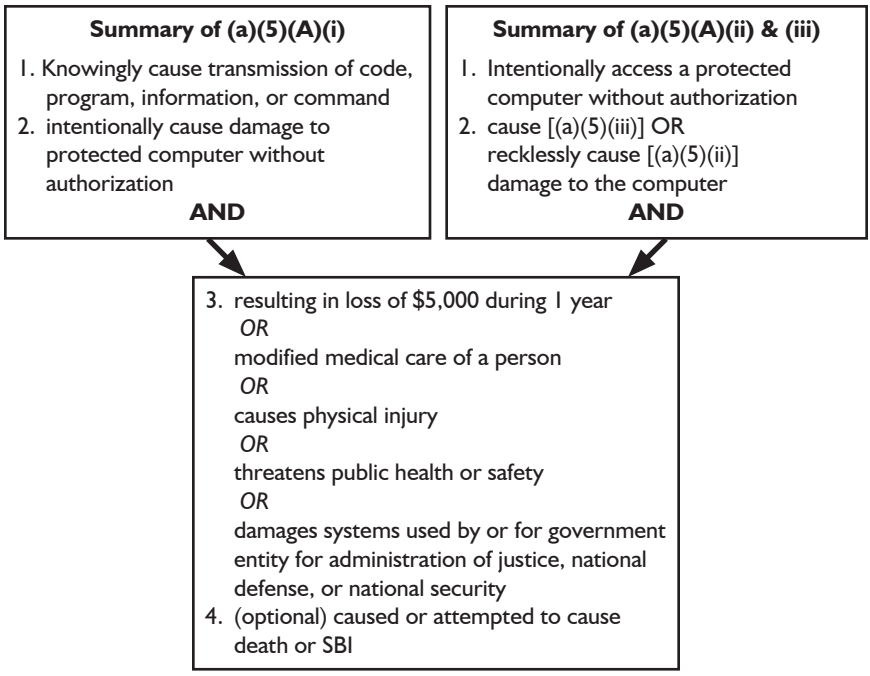
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subsection (A), caused (or, in the case of an attempted offense, would, if completed, have caused)–

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;



> *(iv) a threat to public health or safety; or*
>
> *(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security …*
>
> *shall be punished as provided in subsection (c) of this section.*

The differences between the conduct criminalized by the three subsections of section 1030(a)(5)(A) are important to note. That section criminalizes three different types of conduct, based on mental state and authority to access. In basic terms, subsection (5)(A)(i) prohibits anyone from knowingly damaging a computer (without authorization) while subsection (5)(A)(ii) prohibits unauthorized users from causing damage recklessly and subsection (5)(A)(iii) from causing damage negligently.

The latter two subsections require that the defendant "access" the computer without authorization. These criminal prohibitions hold intruders accountable for any damage they cause while intentionally trespassing on a computer, even if they did not intend to cause that damage. *See* S. Rep. No. 104-357, at 11 (1996), *available at* 1996 WL 492169 (noting that "anyone who knowingly

invades a system without authority and causes significant loss to the victim should be punished ... even when the damage caused is not intentional").

By contrast, section 1030(a)(5)(A)(i) requires proof only of the knowing transmission of something to damage a computer without authorization. The government does not need to prove "access." Because it is possible to damage a computer without "accessing" it, this element is easier to prove (except for the mental state requirement). For example, most worms and trojans spread though self-replication, without personally accessing the affected systems.

1. The Access Element

Subsection (a)(5)(A)(i): Knowingly causing the transmission of a program, information, code, or command to a protected computer

Section 1030(a)(5)(A)(i) prohibits knowingly causing the transmission of a "program, information, code, or command" and as a result of such conduct, *intentionally* causing damage to a protected computer.[5] This subsection applies regardless of whether the offenders were authorized to use the victim computer system (an "insider"), not authorized to use it (an "outsider"), or even those who have never accessed the system at all.

The term "program, information, code, or command" broadly covers all transmissions that are capable of having any effect on a computer's operation. This includes software code, software commands, and network packets designed to exploit system vulnerabilities.

Courts have considered the question of what constitutes knowingly causing the "transmission" of a program, information, code, or command. In the ordinary case where the attacker releases a worm or initiates a denial of service attack, the government should easily meet this element of the crime. On the other hand, this subsection does not apply to "physical" acts that shut down a computer, such as flipping a switch to cut of the electrical supply, as

[5] The earliest versions of § 1030(a)(5) did not establish levels of culpability based on the mental state of the actor vis-à-vis the damage element. The pre-1994 version of the statute, for example, did not require any proof of mental state with respect to the damage caused. *See United States v. Sablan*, 93 F.3d 865, 868-69 (9th Cir. 1996); *United States v. Morris*, 928 F.2d 504, 509 (2d Cir. 1991). As amended in 1994, however, Congress established the mental state test with different treatment for intentional, reckless, and negligent damage. The amendments in 1996 combined these two factors—criminal intent and authority to access—to create a comprehensive scheme. For further discussion of this point, please refer to http://www.cybercrime.gov/1030_analysis.html.

they do not involve transmission of a program or command. Other criminal statutes may cover such conduct, however.

An attacker need not directly send the required transmission in order to violate this statute. In one case, a defendant inserted malicious code into a software program he wrote to run on his employer's computer network. *See United States v. Sullivan*, 40 Fed. Appx. 740 (4th Cir. 2002) (unpublished). After lying dormant for four months, the malicious code activated and downloaded certain other malicious code to several hundred employee handheld computers, making them unusable. *See id.* at 741. The court held that the defendant knowingly caused transmission of code in violation of the statute. *See id.* at 743.

In the civil context, courts have taken the idea of transmission of code even further. In *International Airport Centers, L.L.C. v. Citrin,* the Seventh Circuit held that a civil complaint stated a claim when it alleged that the defendant copied a secure-erasure program to his (company-issued) laptop, and even said in dicta that it made no difference if the defendant copied the program over an Internet connection, from an external disk drive, or an internal disk drive. *International Airport Centers, L.L.C. v. Citrin,* 440 F.3d 418, 419-20 (7th Cir. 2006). Similarly, in *Shaw v. Toshiba America Information Systems*, Toshiba manufactured computers with faulty software that improperly deleted data on diskettes used in their floppy drives, and Toshiba shipped the computers in interstate commerce. *Shaw v. Toshiba America Information Systems,* 91 F. Supp. 2d 926, 931 (E.D. Tex. 1999). In that case, the court found that the shipment of the software by itself constituted its transmission for purposes of the statute. *See id.*[6]

Subsections (a)(5)(A)(ii) or (iii): Intentionally accessed a protected computer without authorization

Subsections 1030(a)(5)(A)(ii) and (iii) require proof that the defendant intentionally accessed a protected computer without authorization. These subsections do not include the phrase "exceeds authorized access." *Compare* 18 U.S.C. § 1030(a)(2) & (a)(4) *with* 18 U.S.C. § 1030(a)(5)(A)(ii) & (iii). Thus, these subsections do not apply to authorized users of a computer who exceed their authorization ("insiders").

[6] Congress later amended § 1030 so that "no [civil] action may be brought ... for the negligent design or manufacture of computer hardware, computer software, or firmware." 18 U.S.C. § 1030(g).

Courts have examined the question of what constitutes unauthorized access for purposes of subsections (a)(5)(A)(ii) and (iii). In many situations the unauthorized access is obvious, such as where an intruder exploits a vulnerability in the security of another person's computer and directly sends commands that cause damage. The courts have also held, however, that an actor may gain "unauthorized access" to a computer by indirect means, such as by releasing an automated, self-replicating program that penetrates the defenses of others' computers. *See United States v. Morris*, 928 F.2d 504, 509-10 (2d Cir. 1991) (defendant obtained "unauthorized access" to computers by releasing a "worm" that copied itself onto many thousands of computers by exploiting security vulnerabilities and guessing passwords).

In ruling on civil suits under section 1030(a)(5), some courts have expanded the idea of "unauthorized access" even further. For example, in one case, a company created an automated program to access its competitor's web server—a publicly available computer—in violation of the competitor's terms of use. *See Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd,* 356 F.3d 393 (2d Cir. 2004). Surprisingly, even though the company that created the automated program did not circumvent any security feature and could lawfully have accessed the site if it did so without using automated programs, the court held that this activity constituted "unauthorized access" for purposes of section 1030(a)(5). *Id*. at 251-52.

Please see page 4 for the discussion of the concept of access without authorization.

2. Cause Damage to the Protected Computer

Section 1030(a)(5) prohibits damaging a computer system. 18 U.S.C. § 1030(a)(5)(A). The statute requires only that the defendant's conduct "cause" damage in a computer. It is not necessary to prove that the damaged protected computer was the same computer that the defendant accessed.

"Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Although this definition is broad and inclusive, as the use of the word "any" suggests, the definition differs in some ways from the idea of damage to physical property. This definition contains several concepts that allow section 1030(a)(5) to apply to a wide variety of situations.

First, "damage" occurs when an act impairs the "integrity" of data, a program, a system, or information. This part of the definition would apply,

for example, where an act causes data or information to be deleted or changed, such as where an intruder accesses a computer system and deletes log files or changes entries in a bank database.

Similarly, "damage" occurs when an intruder changes the way a computer is instructed to operate. For example, installing keylogger software on a home computer can constitute damage. Damage also occurs if an intruder alters the security software of a victim computer so that it fails to detect computer trespassers. For example, in *United States v. Middleton,* part of the damage consisted of a user increasing his permissions on a computer system without authorization. *United States v. Middleton*, 231 F.3d 1207, 1213-14 (9th Cir. 2000).

In addition to the impairment of the integrity of information or computer systems, the definition of damage also includes acts that simply make information or computers "unavailable." Intruders have devised ways to consume all of a computer's computational resources, effectively making it impossible for authorized users to make use of the computer even though none of the data or software has been modified. Similarly, a "denial of service attack" floods a computer's Internet connection with junk data, preventing legitimate users from sending or receiving any communications with that computer. *See YourNetDating v. Mitchell*, 88 F. Supp. 2d 870, 871 (N.D. Ill. 2000) (granting temporary restraining order where defendant installed code on plaintiff's web server that diverted certain users of plaintiff's website to pornography website).

EXAMPLE 1: *Prior to the annual football game between rival schools, an intruder from one high school gains access to the computer system of a rival school and defaces the football team's website with graffiti announcing that the intruder's school was going to win the game.*

In this example, the intruder has caused damage—the integrity of the information on the website has been impaired because viewers of the site will not see the information that the site's designers put there.

EXAMPLE 2: *An attacker configures several thousand computers to access the washingtonpost.com website at the same time in a coordinated denial of service attack. As a consequence, the site is jammed, and for approximately 45 minutes, ordinary web surfers find that the site will not load when they type its URL in their browsers.*

This example also shows damage as defined by the CFAA. The attacker has, via a code or command, impaired the availability of the data on the website to its normal users.

In the computer network world, an intrusion—even a fairly noticeable one—can amount to a kind of trespass that causes no readily discoverable impairment to the computers intruded upon or the data accessed. Even so, such "trespass intrusions" often require that substantial time and attention be devoted to responding to them. In the wake of seemingly minor intrusions, the entire computer system is often audited, for instance, to ensure that viruses, back-doors, or other harmful codes have not been left behind or that data has not been altered or copied. Even adding false information to a computer can impair its integrity. In addition, holes exploited by the intruder are sometimes patched, and the network generally is resecured through a rigorous and time-consuming technical effort. This process can be costly and time-consuming.

> Example 3: *The system administrator of a local community college reviews server logs one morning and notes an unauthorized intrusion that occurred through a backdoor at about 3:30 in the morning. It appears to the administrator that the intruder accessed a student database that listed students' home addresses, phone numbers, and social security numbers. After calling the FBI, she and her staff spend several hours reviewing what occurred, devising patches for the vulnerabilities that were exploited, and otherwise trying to prevent similar intrusions from occurring again. Still, the result of the technical review is that no offending code can be found, and the network appears to function as before. In the two months after the intrusion, staff at the community college report no known alterations or errors in the student database. The cost of the employee time devoted to the review totaled approximately $7,500.*

Although the intruder apparently did not make any alterations to the database and the system seems to work as it did before, in a few civil cases, courts have held that accessing and copying private data may cause damage to the data under the CFAA.[7] *See Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000).

[7] This theory has not been applied in a criminal case. In civil cases, the plaintiff must prove damage under one of the factors in § 1030(a)(5)(B). See page 38 for a list of these factors. Civil plaintiffs do not have § 1030(a)(2) available to them. Therefore, the flexibility courts have shown toward the definition of damage in civil cases may not apply to criminal cases. Further, the trade-secret aspect of *Shurgard* may limit its applicability.

In *Shurgard Storage Centers*, a self-storage company hired away a key employee of its main competitor. Before the employee left to take his new job, he emailed copies of computer files containing trade secrets to his new employer. In support of a motion for summary judgment as to the section 1030(a)(5) count, the defendant argued that the plaintiff's computer system had suffered no "damage" as a consequence of a mere copying of files by the disloyal employee. The court, however, found the term "integrity" contextually ambiguous, and held that the employee did in fact impair the integrity of the data on the system—even though no data was "physically changed or erased" in the process—when he accessed a computer system without authorization to collect trade secrets. *Id*.

Courts have made similar rulings in *HUB Group, Inc. v. Clancy*, 2006 WL 208684 (E.D. Pa. 2006) (downloading employer's customer database to a thumb drive for use at a future employer created sufficient damage to state claim under the CFAA) and *I.M.S. Inquiry Management Systems v. Berkshire Information Systems*, 307 F. Supp. 2d 521, 525-26 (S.D.N.Y. 2004) (allegation that the integrity of copyrighted data system was impaired by defendant's copying it was sufficient to plead cause of action under CFAA).

3. Loss or Other Damage Listed in Section 1030(a)(5)(B)

Section 1030(a)(5) differentiates different types of conduct that cause damage. Section 1030(a)(5)(A) prohibits certain acts when accompanied by particular mental states, while section 1030(a)(5)(B) requires the government to prove that a specific kind of harm resulted from those actions. A violation occurs only where an act meets the elements of *both* subsections.

Thus, in addition to proving one of the subsections of section 1030(a)(5)(A), the government must also prove that one of the harms enumerated in section 1030(a)(5)(B) resulted from the damage. These harms are: (1) at least $5,000 economic loss during a one-year period; (2) an actual or potential effect on medical care; (3) physical injury to a person; (4) a threat to public health or safety; or (5) damage to a computer used in the administration of justice, national defense, or national security. Importantly, the statute does not create a mental state with respect to these resulting harms. The government need not prove that the actor intended to cause any particular one of these harms, but merely that his conduct in fact caused the harm. *See United States v. Suplita*,

Case No. 01cr3650, Order Denying Motion to Dismiss Indictment, at 4 (S.D. Cal. July 23, 2002).[8]

Economic Loss

Of these enumerated harms, the most commonly charged is economic loss. The statute defines "loss" quite broadly: "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). This definition includes, for example, the prorated salary of a system administrator who restores a backup of deleted data, the prorated hourly wage of an employee who checks a database to make sure that no information in it has been modified, the expense of re-creating lost work, the cost of reinstalling system software, and the cost of installing security measures to resecure the computer to avoid further damage from the offender. *See United States v. Middleton*, 231 F.3d 1207, 1213-14 (9th Cir. 2000) (interpreting § 1030(a)(5) before addition of the definition of damage); *see also EF Cultural Travel*, 274 F.3d at 584 n.17 (1st Cir. 2001) (same); *United States v. Sablan*, 92 F.3d 865, 869-70 (9th Cir. 1996) (in calculating "loss" for purposes of earlier version of sentencing guidelines, court properly included standard hourly rate for employees' time, computer time, and administrative overhead).

Loss includes
- Response costs
- Damage assessments
- Restoration of data or programs
- Wages of employees for these tasks
- Lost sales from website
- Lost advertising revenue from website

Loss might include
- Harm to reputation or goodwill
- Other costs if reasonable

Loss does not include
- Assistance to law enforcement

The definition of loss in section 1030(e)(11) is not exclusive and does not preclude other types of financial setbacks that are not specifically listed from being counted toward the $5,000 threshold. Costs that are necessary to restore

[8] Prior to 2001, because the definition of damage contained the "enumerated harms" (now found in § 1030(a)(5)(B)), an argument could be made that the crime required, for example, proof of the intent to cause $5,000 in loss or a threat to public health or safety. By moving these subsections out of the definition of damage, Congress clarified that the government must prove the actor's mental state with respect to damage and not with respect to loss or other harms.

a system to its previous condition are included in any calculation of loss because they are specifically mentioned in section 1030(e)(11). Although money that a victim spends to make a system better or more secure than it was prior to the intrusion may not qualify as "reasonable" in many cases, if the facts of your case suggest otherwise, you should argue to include them.

In meeting the $5,000 loss requirement, the government may aggregate all of the losses to all of the victims of a particular intruder that occur within a one-year period, so long as the losses result from a "related course of conduct." Thus, evidence showing that a particular intruder broke into a computer network five times and caused $1,000 loss each time would meet the statutory requirement, as would $1 loss to 5,000 computers caused by the release of a single virus or worm.[9] In addition, section 1030(e)(12) makes clear that for purposes of establishing loss, the victim can be any natural or legal "person," including corporations, government agencies, or other legal entities.[10]

The statute does not impose a proximate causation requirement on loss or any other of the special harms listed in section 1030(a)(5). Nonetheless, in the *Middleton* opinion the Ninth Circuit noted approvingly that the jury in that case was instructed that the losses claimed had to be a "natural and foreseeable result" of the damage. *Middleton,* 231 F.3d at 1213. This opinion predates the inclusion of a definition of the term "loss" in section 1030. However, given that the statutory definition was modeled on the one used in *Middleton,* prosecutors may be well-advised, if possible, to demonstrate that the losses used to reach the $5,000 threshold were proximately caused by their defendants' actions.

---

[9] Prior to the 2001 amendments, numerous courts struggled with the question of whether and how loss to several victims could be aggregated to meet the $5,000 loss requirement. *See, e.g., Chance v. Avenue A., Inc.,* 165 F. Supp. 2d 1153, 1158 (W.D. Wash. 2001); *Thurmond v. Compaq Computer Corp.*, 171 F. Supp. 2d 667, 680 (E.D. Tex. 2001); *In re America Online, Inc.*, 168 F. Supp. 2d 1359, 1372-73 (S.D. Fla. 2001); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d. 497, 520-25 (S.D.N.Y. 2001). In 2001, Congress clearly settled this issue—at least for criminal proceedings—by amending § 1030(a)(5)(B)(I) to allow aggregation of loss "resulting from a related course of conduct affecting 1 or more other protected computers."

[10] Prior statutory language arguably left open the question of whether a corporation or other legal entity could suffer "loss" for purposes of meeting the $5,000 loss threshold. *See United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000) (rejecting defendant's argument that "individuals" did not include corporations). In 2001, Congress changed the word "individuals" to "persons" and added a broad definition of "person" that includes corporations, government agencies, and any "legal or other entity." 18 U.S.C. § 1030(e)(12).

Because the costs associated with restoring a system to its prior condition are by virtue of the statute reasonable costs, victims should be encouraged to document them carefully. In the event that the intrusion was facilitated by the existence of some known vulnerability—e.g., the operating system had not been patched with the latest security updates—the victim may, understandably, be unwilling to expend funds to restore the system to a state where it is again vulnerable to intrusion. As noted above, however, the fact that a particular cost was incurred in an effort to improve the security of a system is not determinative of whether or not it is properly considered as loss. Rather, the statute defines loss to include "any reasonable cost to the victim." 18 U.S.C. § 1030(e)(11).

Accordingly, the types of losses considered by courts "have generally been limited to those costs necessary to assess the damage caused to the plaintiff's computer system or to resecure the system." *Tyco Int'l v. John Does, 1-3*, 2003 WL 23374767 at *3 (S.D.N.Y. 2003). *See also I.M.S. Inquiry Management Systems v. Berkshire Information Systems*, 307 F. Supp. 2d 521, 526 (S.D.N.Y. 2004) (awarding costs related to "damage assessment and remedial measures"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 584 (1st Cir. 2001) (awarding costs of assessing damage).

"Loss" also includes such harms as lost advertising revenue or lost sales due to a website outage and the salaries of company employees who are unable to work due to a computer shutdown. *See Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 252 n.12 (S.D.N.Y. 2000), *aff'd,* 356 F.3d 393 (2d Cir. 2004) (suggesting, under pre-2001 version of § 1030(a)(5), that lost goodwill and lost profits could properly be included in loss calculations where they result from damage to a computer). In general, the cost of installing completely new security measures "unrelated to preventing further damage resulting from [the offender's] conduct," however, should not be included in the loss total. *See Middleton*, 231 F.3d at 1213; *see also Thurmond v. Compaq Computer Corp.*, 171 F. Supp. 2d 667, 680-83 (E.D. Tex. 2001) (cost of hiring outside consultant to analyze damage "solely in preparation of litigation" may not be included in loss calculation (based on pre-amendment statutory text)). Prosecutors should think creatively about what sorts of harms in a particular situation meet this definition and work with victims to measure and document all of these losses.

At least one court has held that harm to a company's reputation and goodwill as a consequence of an intrusion might properly be considered loss for purposes of alleging a violation of section 1030. *See America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998). *But cf. In Re*

DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 525 n.34 (S.D.N.Y. 2001) (stating that *America Online* is "unpersuasive" and that reputation and goodwill "seem[] far removed from the damage Congress sought to punish and remedy—namely, damage to computer systems and electronic information by intruders").

"Loss" calculations may not include costs incurred by victims primarily to aid the government in prosecuting or investigating an offense. U.S.S.G. § 2B1.1, cmt. n. 3(D)(ii); *United States v. Schuster*, 467 F.3d 614 (7th Cir. 2006).

Medical Care

The second harm in section 1030(a)(5)(B) relates to the "modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment or care of 1 or more individuals." 18 U.S.C. § 1030(a)(5)(B)(ii). This subsection provides strong protection to the computer networks of hospitals, clinics, and other medical facilities because of the importance of those systems and the sensitive data that they contain. This type of special harm does *not* require any showing of financial loss. Indeed, the impairment to computer data caused by an intruder could be minor and easily fixable while still giving rise to justified criminal liability. The evidence only has to show that at least one patient's medical care was at least *potentially* affected as a consequence of the intrusion.

> Example: *A system administrator of a hospital resigns her employment. Before she leaves, she inserts a malicious program into the operating system's code that, when activated one morning, deletes the passwords of all doctors and nurses in the labor and delivery unit. This damage prevents medical personnel from logging on to the computer system, making it impossible to access patients' medical records, charts, and other data. Another system administrator corrects the problem very quickly, restoring the passwords in ten minutes. No patients were in the labor and delivery unit during the incident.*

The conduct in this example should satisfy the "medical" special harm provision. Even though nothing harmful actually occurred as a consequence of the impairment to the system in this case, it requires little imagination to conjure a different outcome where the inability to access the computer system would affect a doctor or nurse's ability to treat a patient. Provided that a medical

professional can testify that a patient's treatment or care could potentially have been modified or impaired, the government can prove this harm.

Physical Injury

The third special harm occurs when the damage to a computer causes "physical injury to any person." 18 U.S.C. § 1030(a)(5)(B)(iii). Computer networks control many other vital systems in our society, such as air traffic control and 911 emergency telephone service. Disruption of these computers could directly result in physical injury.

One issue to consider is whether the chain of causation between the damaged computer and the injury is too attenuated for the court to hold the intruder criminally responsible. Although the statute does not explicitly require that the injury be proximately caused, courts have much experience in applying this sort of test in other areas of the law and might import the doctrine here. So long as there is a reasonable connection between the damaged computer and the injury, however, charging section 1030(a)(5)(B)(iii) is appropriate. For example, suppose that an intruder succeeds in accessing an electric utility's computer system and shuts down power to a three-square-block area, causing the traffic lights to shut down, and a car accident results. If one of the drivers suffers back and neck injuries, the intruder could properly be convicted under this subsection.

Threats to Public Health or Safety

The fourth special harm is closely related to physical harm, but only requires a "threat" to public health or safety. *See* 18 U.S.C. § 1030(a)(5)(B)(iv). Indeed, because the government need not prove actual physical harm to a person, this subsection applies to a wider range of circumstances. Today, computer networks control many of the nation's critical infrastructures, such as electricity and gas distribution, water purification, nuclear power, and transportation. Damage to the computers that operate these systems or their control and safety mechanisms can create a threat to the safety of many people at once.

Justice, National Defense, or National Security

Finally, the "special harm" requirement can be satisfied if the damage affects "a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. § 1030(a)(5)(B)(v). In 2001, Congress added this subsection because

this sort of damage can affect critically important functions—such as one intruder's attempt to access a court computer without authority and change his sentence—but may not be easily quantified in terms of economic loss under § 1030(a)(5)(B)(i).

Here, "the administration of justice" includes court system computers, but would also appropriately extend to computers owned by state or federal law enforcement agencies, prosecutors, and probation offices. Similarly, computers used "in furtherance of ... national defense, or national security" would include most computer networks owned by the Department of Defense. The statutory language does not require that the computer be owned or operated by the government—computers owned by a defense contractor, for example, could be "used ... for" the military in furtherance of national security. At the same time, not every Defense Department computer is used "in furtherance" of the national defense. A computer at the cafeteria in the Pentagon might not qualify, for example.

4. Penalties

Section 1030(a)(5)(A) sets forth three mental states for the causing of damage, with varying penalty levels for each. Where the individual acts intentionally, the maximum sentence is ten years' imprisonment. 18 U.S.C. § 1030(c)(4)(A). If the individual accesses a protected computer without authorization and recklessly causes damage under subsection (5)(A)(ii), the maximum sentence is five years in prison. 18 U.S.C. § 1030(c)(4)(B). In either case, if the offense follows a conviction for *any* crime under section 1030, the maximum sentence rises to 20 years' imprisonment. § 1030(c)(4)(C). If the attacker accesses a computer without authorization and causes damage with no culpable mental state (i.e., accidentally or negligently), the crime is a misdemeanor with a maximum penalty of one year imprisonment. 18 U.S.C. § 1030(c)(2)(A). But, violations of section 1030(a)(5)(A)(iii) that follow a previous conviction under section 1030 result in a ten year maximum penalty. 18 U.S.C. § 1030(c)(3)(B).

In 2002, Congress added an additional sentencing provision that raised the maximum penalties for certain of these crimes that result in serious bodily injury or death. If the offender intentionally damages a protected computer under § 1030(a)(5)(A)(i) and "knowingly or recklessly causes or attempts to cause serious bodily injury," the maximum penalty rises to 20 years' imprisonment,

and where the offender knowingly or recklessly causes or attempts to cause death, the court may impose life in prison. *See* 18 U.S.C. § 1030(c)(5).

TABLE 3. PENALTY SUMMARY FOR SECTION 1030(A)(5)(A)

Section	Statutory Penalty
Intentional Damage § 1030(a)(5)(A)(i)	10-year felony 20-year felony for subsequent convictions or serious bodily injury Life imprisonment if offender causes or attempts to cause death
Reckless Damage § 1030(a)(5)(A)(ii)	5-year felony 20-year felony for subsequent convictions
Damage § 1030(a)(5)(A)(iii)	Misdemeanor 10-year felony for subsequent convictions

5. Relation to Other Statutes

In many cases, intruders cause damage to systems even though their primary intent is to steal information or commit a fraud in violation of sections 1030(a)(2) or (a)(4). For example, intruders commonly try to make it difficult for system administrators to detect them by erasing log files that show that they accessed the computer network. Deleting these files constitutes intentional "damage" for purposes of section 1030(a)(5). Similarly, intruders commonly modify system programs or install new programs to circumvent the computer's security so that they can access the computer again later. This activity impairs the integrity of the computer and its programs and therefore meets the damage requirement. As long as the government can meet one of the other requirements under § 1030(a)(5)(B)—such as $5,000 in loss, or damage that affects a computer used in furtherance of the national defense—a charge under § 1030(a)(5) is appropriate in addition to any other charges under § 1030.

Prosecutors should also consider section 1030(a)(5) in cases where an individual breaks into a federal government computer in violation of § 1030(a)(3), a misdemeanor. If the act causes damage, as well as causes one of the enumerated harms, prosecutors may be able to charge one of the felony offenses in § 1030(a)(5).

When faced with conduct that damages a protected computer, prosecutors should also consider several other statutes that punish the same conduct when particular circumstances are present. For example, where the criminal act causes

damage to a computer for communications that is "operated or controlled by the United States," or "used or intended to be used for military or civil defense functions," prosecutors should consider charging 18 U.S.C. § 1362, a ten-year felony. Other potentially applicable statutes are discussed in Chapter 3, "Other Network Crime Statutes."

6. Background

Prior to the USA PATRIOT Act, the CFAA contained no definition of loss. The definition was left to the purview of the courts.

In *United States v. Middleton*, 231 F.3d 1207 (9th Cir. 2000), the Ninth Circuit was asked to rule upon the question of how to define the term "loss" in establishing a violation of section 1030(a)(5). In that case, the defendant was accused of gaining unlawful access to an ISP's computer network, changing administrative passwords, altering the computer's registry, and deleting several databases. *See id.* at 1209. Two employees of the ISP spent an entire weekend repairing the damage and restoring data, and spent many additional hours investigating the source and extent of the damage that was caused. In addition, the ISP hired an outside consultant for technical support, and purchased some new software to replace some that the defendant had deleted. The government contended that all of these expenses together constituted a total loss of $10,092 to the victim ISP—though employee time computed at an hourly rate based on their respective annual salaries made up the bulk of that amount.

The jury rendered a guilty verdict and the defendant challenged the sufficiency of the evidence because the trial court had permitted employee time to be included in the "loss" calculation, without which the $5,000 threshold would not have been reached. The appellate court upheld the conviction, finding no abuse of discretion in the district court's broad definition of "loss." In particular, the appellate court upheld the district court's jury instructions, which stated that the jury "may consider what measures were reasonably necessary to restore the data, program, system, or information that … was damaged or what measures were reasonably necessary to resecure the data, program, system, or information from further damage." *Id.* at 1213. The jury instructions also stated that the jury "may consider any loss that … was a natural and foreseeable result of any damage that … occurred." *Id.*

The USA PATRIOT Act essentially adopted the *Middleton* court's definition of loss in 18 U.S.C. § 1030(e)(11). The term "loss" is now defined by statute to include "any reasonable cost to any victim, including the cost of

responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." The government must still prove that the costs incurred are reasonable ones.

G. Trafficking in Passwords: 18 U.S.C. § 1030(a)(6)

Section 1030(a)(6) prohibits a person from knowingly and with intent to defraud trafficking in computer passwords and similar information when the trafficking affects interstate or foreign commerce, or when the password may be used to access without authorization a computer used by or for the federal government. First offenses of this section are misdemeanors.

Summary

1. Trafficking
2. in computer password or similar information
3. knowingly and with intent to defraud
4. trafficking affects interstate or foreign commerce
   OR
   computer used by or for U.S.

Title 18, United States Code, Section 1030(a)(6) provides:

Whoever–

(6) Knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if–

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States ….

shall be punished as provided in subsection (c) of this section.

1. Trafficking

The term "traffic" in section 1030(a)(6) is defined by reference to the definition of the same term in 18 U.S.C. § 1029, which means "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. § 1029(e)(5). A profit motive is not required. However, the definition excludes mere possession of passwords if the defendant has no intent to transfer or dispose of them. *Id.* Similarly, personal use of

an unauthorized password is not a violation of section 1030(a)(6), although it may be a violation of other provisions under section 1030 that apply to unauthorized access to computers or of section 1029.

2. Password or Similar Information

The term "password" does not mean just a single word or phrase that enables one to access a computer. The statute prohibits trafficking in passwords *or similar information:*

> The Committee recognizes that a "password" may actually be comprised of a set of instructions or directions for gaining access to a computer and intends that the word "password" be construed broadly enough to encompass both single words and longer more detailed explanations on how to access others' computers.

S. Rep. No. 99-432, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2491. Therefore, prosecutors should apply the term "password" using a broad meaning to include any instructions that safeguard a computer. Pass phrases, codes, usernames, or any other method or combination of methods by which a user is authenticated to a computer system may qualify as a password under section 1030(a)(6).

3. Knowingly and With Intent to Defraud

For a discussion of this phrase in section 1030(a)(4), please see page 23.

4. Trafficking Affects Interstate or Foreign Commerce

For a violation of subsection (A), the trafficking must affect interstate or foreign commerce. The phrase "affects interstate or foreign commerce" is not statutorily defined or interpreted in case law. However, courts have typically construed this requirement expansively when interpreting other statutes that require a certain conduct to affect interstate or foreign commerce. For example, the United States Court of Appeals for the Ninth Circuit held that a defendant's illicit possession of out-of-state credit card account numbers is an offense "affecting interstate or foreign commerce" within the meaning of section 1029. *United States v. Rushdan*, 870 F.2d 1509, 1514 (9th Cir. 1989). In a similar vein, the United States Court of Appeals for the Sixth Circuit held that a fraudulent credit card transaction affects interstate commerce for purposes of section 1029, inasmuch as banking channels were used for gaining

authorization for the charges. *United States v. Scartz*, 838 F.2d 876, 879 (6th Cir. 1988).

5. Computer Used By or For the U.S. Government

To prove a violation of subsection (B), the password or similar information must be for accessing without authorization a computer used by or for the federal government. Reference to a computer "used by or for the Government of the United States" (also found in section 1030(a)(3)) is not defined by statute or case law, but by its plain meaning should encompass any computer used for official business by a federal government employee or on behalf of the federal government.

6. Penalties

Violations of section 1030(a)(6) are misdemeanors punishable by a fine or a one-year prison term for the first offense. *See* 18 U.S.C. § 1030(c)(2)(A). If the defendant has a previous conviction under section 1030, the maximum sentence increases to ten years' imprisonment. *See* 18 U.S.C. § 1030(c)(2)(C).

7. Relation to Other Statutes

Given the shared statutory definition, section 1030(a)(6) cases often overlap with access device cases under section 1029. Passwords are also access devices under section 1029. *See, e.g., United States v. Fernandez*, 1993 WL 88197 (S.D.N.Y. 1993) (holding that the plain meaning of the term "access device" covers "stolen and fraudulently obtained passwords which may be used to access computers to wrongfully obtain things of value"). For more information on section 1029, see Chapter 3, "Other Network Crime Statutes."

8. Historical Notes

Congress enacted section 1030(a)(6) in 1986 as a "misdemeanor offense aimed at penalizing conduct associated with 'pirate bulletin boards,' where passwords are displayed that permit unauthorized access to others' computers." S. Rep. No. 99-432, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2490.

H. Threatening to Damage a Computer: 18 U.S.C. § 1030(a)(7)

Section 1030(a)(7), which prohibits extortion threats to damage a computer, is the high-tech variation of old-fashioned extortion. This section applies, for example, to situations in which intruders threaten to penetrate a system and encrypt or delete a database. Other scenarios might involve the threat of distributed denial of service attacks that would shut down the victim's computers. Section 1030(a)(7) enables the prosecution of modern-day extortionists who threaten to harm or damage computer networks—without causing physical damage—unless their demands are met.

Title 18, United States Code, Section 1030(a)(7) provides:

Whoever–

(7) With intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer ...

shall be punished as provided in subsection (c) of this section.

Summary

1. With intent to extort money or any other thing of value
2. transmits in interstate or foreign commerce a communication
3. containing a threat to damage a protected computer

1. Intent to Extort Money or Other Thing of Value

In order to prove the "intent to extort" element, it is not necessary to prove that the defendant actually succeeded in obtaining the money or thing of value, or that the defendant actually intended to carry out the threat made. Extortion generally refers to the intent to obtain money or other thing of value with a person's consent induced by the wrongful use of actual or threatened fear, violence, or force.

2. Transmit Communication In Interstate or Foreign Commerce

The extortion threat must be transmitted in interstate or foreign commerce. However, the threat need not be sent electronically. Rather, the statute covers "any interstate or international transmission of threats against computers, computer networks, and their data and programs where the threat is received by mail, a

telephone call, electronic mail, or through a computerized messaging service." *See* S. Rep. No. 104-357, at 12 (1996), *available at* 1996 WL 492169.

3. Threat to Cause Damage to a Protected Computer

The term "damage" is defined in section 1030(e)(8) and is discussed in the context of section 1030(a)(5) on page 34. Unlawful threats to cause damage include interference in any way with the normal operation of the computer or system in question, including denying access to authorized users, erasing or corrupting data or programs, slowing down the operation of the computer or system, or encrypting data and demanding money for the decryption key. *See* S. Rep. No. 104-357, at 12 (1996), *available at* 1996 WL 492169. In contrast, unlawful threats to the business that owns the computer system, such as threats to reveal flaws in the network, or reveal that the network has been hacked, are not threats to a protected computer under section 1030(a)(7). However, a threat to a business, rather than to a protected computer, is a classic example of a violation of the Hobbs Act, 18 U.S.C. § 1951.

The term "protected computer" is defined in section 1030(e)(2) and is discussed in the "Key Definitions" on page 3.

4. Penalties

A violation of section 1030(a)(7) is punishable by a fine and up to five years in prison. 18 U.S.C. § 1030(c)(3)(A). If the defendant has a previous conviction under section 1030, the maximum sentence increases to 10 years' imprisonment. 18 U.S.C. § 1030(c)(3)(B).

5. Relation to Other Statutes

The elements of section 1030(a)(7) generally parallel the elements of a Hobbs Act (18 U.S.C. § 1951, interference with commerce by extortion) violation with some important differences. First, the intent to extort from any person money or other thing of value is the same under section 1030(a)(7) and under section 1951. However, in contrast to section 1951, section 1030(a)(7) does not require proof that the defendant delayed or obstructed commerce. Proving that the threat was transmitted in interstate or foreign commerce is sufficient.

At least one case has recognized the similarities between the two statutes. In *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001), the defendant hacked into the victim's network and obtained root access to the victim's

servers. He then proposed that the victim hire him as a "security expert" to prevent further security breaches, including the deletion of all of the files on the server. Without much discussion, the court determined that the analysis under section 1030(a)(7) was the same as that for the Hobbs Act. *See id.* at 372.

6. Historical Notes

Congress added section 1030(a)(7) to the CFAA in 1996 to fill perceived gaps in the application of existing anti-extortion statutes:

> These cases, although similar in some ways to other cases involving extortionate threats directed against persons or property, can be different from traditional extortion cases in certain respects. It is not entirely clear that existing extortion statutes, which protect against physical injury to persons or property, will cover intangible computerized information.
>
> For example, the "property" protected under existing laws, such as the Hobbs Act, 18 U.S.C. 1951 (interference with commerce by extortion) or 18 U.S.C. 875(d) (interstate communication of a threat to injure the property of another), does not clearly include the operation of a computer, the data or programs stored in a computer or its peripheral equipment, or the decoding keys to encrypted data.

S. Rep. No. 104-357, at 12 (1996), *available at* 1996 WL 492169.

I. Legislative History

From 1996 until the passage of the USA PATRIOT Act in 2001, Section 1030(e)(8) had defined "damage" to mean:

> any impairment to the integrity or availability of data, a program, a system, or information, that–
>
> (A) causes loss aggregating at least $5,000 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; or
>
> (D) threatens public health or safety ….

Under that version of the statute—the version that was in effect at the time of the *Shurgard* decision—a violation of section 1030(a)(5) required that damage be proved in one of four ways; proving loss in excess of $5,000 was one of the ways of proving damage.

An earlier version of the statute that was in effect between 1994 and 1996, required proof of both "damage" *and* "loss" to show a violation of section 1030.[11] Congress amended the statute in 1996 to the version that was in effect at the time of the *Shurgard* decision. The 1996 amendments changed the definition of "damage" as set forth above to mean impairment that *causes* loss or other harms. As the *Shurgard* opinion noted, in the 1996 amendments Congress equated damage and loss to address situations wherein monetary loss might be demonstrated but other forms of damage might be difficult to demonstrate. In the Senate Report accompanying the 1996 amendments to the statute, Congress gave the following example as justification for the change:

> The 1994 amendment required both "damage" and "loss," but it is not always clear what constitutes "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the intruders can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. *Arguably, in such a situation, neither the computer*

[11] In 1995, 18 U.S.C. § 1030(a)(5) (emphasis added) read as follows:

Whoever–

(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if–

(i) the person causing the transmission intends that such transmission will

(I) *damage, or cause damage to, a computer, computer system, network, information, data, or program*; or

(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program; *and*

(ii) the transmission of the harmful component of the program, information, code, or command–

(I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

(II)(aa) *causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period;* or

(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals….

> *nor its information is damaged*. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to securing the system. *Thus, although there is arguably no "damage," the victim does suffer "loss."* If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.
>
> The bill therefore defines "damage" in new subsection 1030(e)(8), with a focus on the harm that the law seeks to prevent.

Shurgard, 119 F. Supp. 2d at 1126 (*citing* S. Rep. No. 104-357, at 11 (1996), *available at* 1996 WL 492169) (emphasis added).

According to this view, Congress wanted to recognize a criminal or civil cause of action when a victim incurred significant response costs as a result of an intrusion, even where no data was changed and the computer functioned as before. Accordingly, Congress defined "damage" to include the causation of loss in excess of a certain threshold amount ($5,000) or other special harms, such as physical injury to any person. With this understanding, the password sniffer example in the Senate Report, as well as the community college intrusion example discussed on page 36, were each likely subject to prosecution from 1996 through 2001 provided the $5,000 monetary threshold of "loss" was met.

Chapter 2
Wiretap Act

The Wiretap Act, often referred to as "Title III," has as its dual purposes: "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153; *see also In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications"). Although the original act covered only wire and oral communications, Congress amended it in 1986 to include electronic communications. *See Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995) ("The principal purpose of the 1986 amendments to Title III was to extend to 'electronic communications' the same protections against unauthorized interceptions that Title III had been providing for 'oral' and 'wire' communications via common carrier transmissions"). The 1986 amendments make the Wiretap Act another option for prosecuting computer intrusions that include real-time capture of information.

Because this manual focuses on prosecution of criminal offenses, this chapter only addresses the first of the Wiretap Act's two purposes, protecting the privacy of communications. For more on law enforcement's access to information concerning communications, see U.S. Department of Justice, *Searching and Seizing Computers and Electronic Evidence in Criminal Investigations* (Office of Legal Education 2002). Also, in keeping with the manual's focus on computer crimes, this section highlights Title III's applicability in that context and does not address every type of case covered by the Act.[1]

[1] Section 2511(1)(b) applies only to certain interceptions of oral communications, i.e., communications that are "uttered by a person" and are not electronic communications. *See* 18 U.S.C. § 2510(2) (definition of "oral communication"). Accordingly, section 2511(1)(b) generally will not apply to network intrusions, which almost always involve electronic communications, and that section is not discussed here.

A. Intercepting a Communication: 18 U.S.C. § 2511(1)(a)

Summary

1. Intentional
2. interception (or endeavoring or procuring another to intercept)
3. of the contents
4. of a wire, oral or electronic communication
5. by use of a device

The core prohibition of the Wiretap Act is found at section 2511(1)(a), which prohibits any person from intentionally intercepting, or attempting to intercept, any wire, oral, or electronic communication." When the requirements of the defined terms are taken into account, a violation of this section has five elements. *See In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 18 (1st Cir. 2003).

Title 18, United States Code, Section 2511(1)(a) provides:

Except as otherwise specifically provided in this chapter any person who–

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication ….

shall be punished as provided in subsection (4).

1. Intentional

Since the 1986 amendments, in order to constitute a criminal violation, the interception of a covered communication must be "intentional"—deliberate and purposeful. *See United States v. Townsend*, 987 F.2d 927, 930 (2d Cir. 1993). In those amendments, Congress deliberately changed the mens rea requirement from "willfully" to "intentionally." *See* S. Rep. No. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

Although a defendant must have intended to intercept a covered communication, he or she need not have specifically intended to violate the Wiretap Act. In other words, a mistake of law is not a defense to a Wiretap Act charge. *See Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 178-79 (5th Cir. 2000); *Reynolds v. Spears*, 93 F.3d 428, 435-36 (8th Cir. 1996) (holding that reliance on incorrect advice from law enforcement officer is not a defense); *Williams v. Poulos*, 11 F.3d 271, 285 (1st Cir. 1993) (rejecting a good faith defense where defendant mistakenly believed his use and disclosure was authorized by the statute); *Thompson v. Dulaney*, 970 F.2d 744, 749 (10th Cir. 1992) (noting

that a "defendant may be presumed to know the law"); *Heggy v. Heggy*, 944 F.2d 1537, 1541-42 (10th Cir. 1991) (rejecting a "good faith" defense based upon a mistake of law).

2. Interception

The Wiretap Act defines an "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device." 18 U.S.C. § 2510(4). This statutory definition does not explicitly require that the "acquisition" of the communication be *contemporaneous* with the transmission of the communication. However, a contemporaniety requirement is necessary to maintain the proper relationship between the Wiretap Act and the Electronic Communications Privacy Act's restrictions on access to stored communications.

Most courts addressing the potential overlap between the two acts have held that both wire and electronic communications are "intercepted" within the meaning of the Wiretap Act only when such communications are acquired contemporaneously with their transmission. An individual who obtains access to a stored copy of the communication does not "intercept" the communication. *See, e.g., Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 460-63 (5th Cir. 1994) (access to stored email communications); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876-78 (9th Cir. 2002) (website); *Wesley College v. Pitts*, 974 F. Supp. 375, 384-90 (D. Del. 1997) (email); *United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990) (pager communications); *United States v. Reyes*, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (same); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (same); *United States v. Moriarty*, 962 F. Supp. 217, 220-21 (D. Mass. 1997) (stored wire communications); *In re State Police Litigation*, 888 F. Supp. 1235, 1264 (D. Conn. 1995) (same); *Payne v. Norwest Corp.*, 911 F. Supp. 1299, 1303 (D. Mont. 1995) (same), *aff'd in part and rev'd in part*, 113 F.3d 1079 (9th Cir. 1997) (same).

A divided panel of the First Circuit took this line of reasoning to an extreme in an opinion later withdrawn by the First Circuit after rehearing the case en banc. *See United States v. Councilman*, 373 F.3d 197 (1st Cir.), *rehearing en banc granted and opinion withdrawn*, 385 F.3d 793 (1st Cir. 2004), *reversed on rehearing en banc*, 418 F.3d 67 (1st Cir. 2005). In *Councilman*, a divided panel of the First Circuit affirmed the dismissal of the indictment for conspiracy to wiretap electronic mail messages. 373 F.3d at 197. The defendant was charged

with acquiring the email messages contemporaneously with their transmission. The indictment alleged that before email messages were ultimately delivered to customers, the defendant's software program made copies of the messages from the servers that were set up to deliver the messages. Two of the three judges agreed with dicta from earlier cases that such email messages acquired from a computer's random access memory (RAM) or hard disk are outside the scope of the Wiretap Act. *Id.* On rehearing en banc, the First Circuit reversed the panel decision, holding that email in electronic storage can be intercepted electronic communications when acquired contemporaneously with their transmission. 418 F.3d at 67.

Notwithstanding the ultimate reversal on the panel's decision in *Councilman*, any prosecutor outside the First Circuit confronting an interception involving acquisition of information from any type of computer memory should anticipate the possibility of a *Councilman* defense. This may apply to prosecutions of spyware users and manufacturers, intruders using packet sniffers, or persons improperly cloning email accounts. Defendants accused of these types of interceptions may argue that the communications they acquired were "in electronic storage" at the time of acquisition, and therefore were not intercepted under Title III.

Even with the possibility of a *Councilman*-type defense, prosecutors should continue to charge violations of section 2511(1)(a) when an individual acquires the contents of a communication contemporaneously with its transmission or in a manner that is effectively contemporaneous with transmission. If a *Councilman*-type argument appears to apply to a prosecution, prosecutors are encouraged to contact CCIPS at (202) 514-1026. Prosecutors may also consider charging violation of section 2701(a) (access to communications residing in an electronic communication service provider facility) for unread email messages or section 1030(a)(2)(C) (unauthorized access to and obtaining information from protected computers) in addition to the Wiretap Act.

3. Contents of a Communication

To be an interception, the acquisition must be of the *contents* of the communication. 18 U.S.C. § 2510(4). "'[C]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Congress amended the definition in 1986 to "distinguish[] between the substance, purport or meaning of the communication and the

existence of the communication or transactional records about it." S. Rep. No. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567.

Some types of information concerning network communications, such as full-path URLs, may raise arguments about whether they contain content. We encourage prosecutors who have questions about whether a particular type of information constitutes "contents" under the Wiretap Act to contact CCIPS for assistance at (202) 514-1026.

4. Wire, Oral, or Electronic Communication

The Wiretap Act prohibits the interception of "any wire, oral or electronic communication." 18 U.S.C. § 2511(1)(a). Each of the three types of communications covered by the Wiretap Act is separately defined by the statute. *See* 18 U.S.C. § 2510(1) (wire), (2) (oral), & (12) (electronic). Typically, network communications that do not contain the human voice will fall into the broad catch-all category of "electronic communications." *See* S. Rep. 99-541, at 14 ("As a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice").

An "electronic communication" is "any transfer ... transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). In the context of network crimes, some defendants may attempt to convince courts to parse an intercepted communication into separate "transfers" in order to have their conduct excluded from this definition of an "electronic communication."

For instance, a defendant has claimed that his device that acquired transfers between a keyboard and a computer did not acquire any electronic communications. *United States v. Ropp,* 347 F. Supp. 2d 831 (C.D. Cal. 2004). In *Ropp*, the defendant placed a piece of hardware between the victim's computer and her keyboard that recorded the signals transmitted between the two. *Id.* The court dismissed the indictment charging a violation of section 2511 because it found that the communications that were acquired were not "electronic communications" within the meaning of the statute. *Id.* The court concluded that "the communications in question involved preparation of emails and other communications, but were not themselves emails or any other communication at the time of the interception." *Id.* at 835 n.1. Because the court found that the typing was a communication "with [the victim's] own computer," it reasoned

that "[a]t the time of interception, [the communications] no more affect[] interstate commerce than a letter, placed in a stamped envelope, that has not yet been mailed." *Id*.

Notwithstanding the *Ropp* decision, prosecutors should pursue cases involving interceptions occurring on computers or internal networks that affect interstate commerce. For example, if an individual installs malicious software on the victim's computer that makes a surreptitious copy every time an email is sent, or captures such messages as they move on the local area network on their way to their ultimate destination half way around the world, such cases can be prosecuted under section 2511.

The text of section 2511 and the statute's legislative history support this interpretation. A transfer should include all transmission of the communication from the originator to the recipient. First, the plain text of the definition of "electronic communication" is incompatible with such a piecemeal approach. The definition explicitly contemplates that a "transfer" may be transmitted by a system "in whole or in part." If "transfer" were meant to refer to each relay between components on a communication's journey from originator to recipient, no system could be said to transmit a transfer "in part." In addition, the legislative history of the 1986 amendments that added the term "electronic communication" provides some useful explanation. The House Report explicitly states that "[t]o the extent that electronic and wire communications passing through [customer equipment] affect interstate commerce, the Committee intends that those communications be protected under section 2511." H.R. Rep. No. 99-647, at 33. Similarly, the Senate Report discusses the inclusion of communications on private networks and intracompany communications systems. *See* S. Rep. No. 99-541, at 12, *reprinted in* 1968 U.S.C.C.A.N. 3555, 3566. In these discussions, Congress explicitly rejected the premise that acquiring a communication on the customer's own equipment would take it out of the protections of the Wiretap Act. *See* H.R. Rep. No. 99-647, at 33 (discussing interceptions occurring at customer's premises on customer equipment connected to public or private communications networks and making clear that such interceptions violate the Act).

5. Use of a Device

Finally, to be an interception under the Act, the acquisition must be by use of an "[e]lectronic, mechanical or other device." 18 U.S.C. § 2510(4). Generally, "'electronic, mechanical or other device' means any device or apparatus which

can be used to intercept a wire, oral, or electronic communication" subject to two specific exceptions. 18 U.S.C. § 2510(5).

The little existing case law on what constitutes a device focuses on the exceptions to the rule, rather than on what actually qualifies as a device. *See, e.g., Adams v. Sumner*, 39 F.3d 933 (9th Cir. 1994). In a typical network crime, the device used could be the computer that is used to intercept the communication or a software program running on such a computer. Each appears to satisfy the statutory requirements. *See* 18 U.S.C. § 2510(5).

The definition of device explicitly excludes (1) equipment used in the ordinary course of service (e.g., a telephone used for telephone service) and (2) hearing aids used to "correct subnormal hearing to not better than normal." *Id.* In addition, the "extension telephone" exception excludes:

> any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

18 U.S.C. § 2510(5)(a). Congress intended this exception to have a fairly narrow application: the exception was designed to permit businesses to monitor by way of an "extension telephone" the performance of their employees who spoke on the phone to customers. The "extension telephone" exception makes clear that when a phone company furnishes an employer with an extension telephone for a legitimate work-related purpose, the employer's monitoring of employees using the extension phone for legitimate work-related purposes does not violate Title III. *See Briggs v. American Air Filter Co.*, 630 F.2d 414, 418 (5th Cir. 1980) (reviewing legislative history of Title III); *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (applying exception to permit monitoring of sales representatives); *James v. Newspaper Agency Corp*. 591 F.2d 579, 581 (10th Cir. 1979) (applying exception to permit monitoring of newspaper employees' conversations with customers).

The case law interpreting the extension telephone exception is notably erratic, largely owing to the ambiguity of the phrase "ordinary course of business." Some courts have interpreted "ordinary course of business" broadly to mean "within the scope of a person's legitimate concern," and have applied the extension telephone exception to contexts such as intrafamily disputes. *See, e.g., Simpson v. Simpson*, 490 F.2d 803, 809 (5th Cir. 1974) (holding that husband did not violate Title III by recording wife's phone calls); *Anonymous v. Anonymous*, 558 F.2d 677, 678-79 (2d Cir. 1977) (holding that husband did not violate Title III in recording wife's conversations with their daughter in his custody). Other courts have rejected this broad reading, and have implicitly or explicitly excluded surreptitious activity from conduct within the "ordinary course of business." *See Kempf v. Kempf*, 868 F.2d 970, 973 (8th Cir. 1989) (holding that Title III prohibits all wiretapping activities unless specifically excepted and that the Act does not have an express exception for interspousal wiretapping); *United States v. Harpel*, 493 F.2d 346, 351 (10th Cir. 1974) ("We hold as a matter of law that a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business"); *Pritchard v. Pritchard*, 732 F.2d 372, 374 (4th Cir. 1984) (rejecting view that § 2510(5)(a) exempts interspousal wiretapping from Title III liability). Some of the courts that have embraced the narrower construction of the extension telephone exception have stressed that it permits only limited work-related monitoring by employers. *See, e.g., Deal v. Spears*, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that employer monitoring of employee was not authorized by the extension telephone exception in part because the scope of the interception was broader than that normally required in the ordinary course of business).

On top of the ambiguities concerning the contours of this carve-out from the definition of device, it is not at all clear that this exception would transfer to the network crime context. While computers may qualify as equipment or facilities, whether "telephone or telegraph" modifies all three types of objects, i.e., "instrument, equipment or facility," or only instruments, is not yet settled.

Moreover, the exception in section 2510(5)(a)(ii) that permits the use of "any telephone or telegraph instrument, equipment or facility, or any component thereof" by "an investigative or law enforcement officer in the ordinary course of his duties" is a common source of confusion. This language does *not* permit agents to intercept the private communications of the targets

of a criminal investigation on the theory that a law enforcement agent may need to intercept communications "in the ordinary course of his duties." As Chief Judge Posner explained:

> Investigation is within the ordinary course of law enforcement, so if "ordinary" were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent. Since the purpose of the statute was primarily to regulate the use of wiretapping and other electronic surveillance for investigatory purposes, "ordinary" should not be read so broadly; it is more reasonably interpreted to refer to routine non investigative recording of telephone conversations .... Such recording will rarely be very invasive of privacy, and for a reason that does after all bring the ordinary-course exclusion rather close to the consent exclusion: what is ordinary is apt to be known; it imports implicit notice.

Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999). For example, routine taping of all telephone calls made to and from a police station may fall within this law enforcement exception, but non-routine taping designed to target a particular suspect ordinarily would not. *See id.*; *accord United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002) (concluding that routine recording of calls made from prison falls within law enforcement exception); *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (same).

B. Disclosing an Intercepted Communication: 18 U.S.C. § 2511(1)(c)

Summary

1. Intentional disclosure
2. of Illegally intercepted communication
3. knowledge or reason to know the intercept was illegal

The Wiretap Act prohibits not only the interception of communications, but also the intentional disclosure of communications that are known to have been illegally intercepted. 18 U.S.C. § 2511(1)(c).

Title 18, United States Code, Section 2511(1)(c) provides:

> *Except as otherwise specifically provided in this chapter any person who–*
>
> *(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception*

of a wire, oral, or electronic communication in violation of this subsection ….

shall be punished as provided in subsection (4).

1. Intentional Disclosure

While the statute unquestionably covers the disclosure of the actual contents of a communication, courts have interpreted the disclosure prohibition more broadly. *See Deal v. Spears*, 780 F. Supp. 618, 624 (W.D. Ark. 1991) (finding liability for disclosure when only the "nature" of the communications was disclosed), *aff'd*, 980 F.2d 1153 (8th Cir. 1992). However, disclosure of the mere fact that an illegal interception took place does not violate the prohibition on disclosure of the contents of intercepted communications. *See Fultz v. Gilliam*, 942 F.2d 396, 403 (6th Cir. 1991). In addition, disclosure of the contents of an intercepted communication that has already become "public information" or "common knowledge" is not prohibited. *See* S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2181.

2. Illegal Interception of Communication

Generally, there can be no illegal disclosure of an illegally intercepted communication without an underlying violation of section 2511(1)(a). Although the defendant need not be the individual who intercepted the communication, in most cases the prosecution must prove that someone intercepted a covered communication in violation of section 2511(1)(a), covered above.

The Senate Report suggests an exception to the general rule that section 2511(1)(a) must have been violated. If a communication is intercepted, but the interception does not violate section 2511(1)(a) only because the interception was not intentional, the Senate Report states that use or disclosure of the communication would still violate the Act. *See* S. Rep. No. 99-541, at 25 (1986), *reprinted in* 1968 U.S.C.C.A.N. 3555, 3579.

3. Knowledge of the Illegal Interception

The prosecution must also prove that the disclosing individual knew or had reason to know that the "information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." 18 U.S.C. § 2511(1)(c). As with section 2511(1)(a), mistake of law is not a defense in that the prosecution need show only that the defendant knew the relevant facts, not that the defendant knew that the interception was in fact

unlawful. *See United States v. Wuliger*, 981 F.2d 1497, 1501 (6th Cir. 1992); *see also Williams v. Poulos*, 11 F.3d 271, 284-85 (1st Cir. 1993). However, a prosecutor should be prepared to defeat any claim that the defendant was mistaken about any fact that would have authorized the interception. *See id.*

4. First Amendment Limitation

Although the prohibition on disclosure is broad, the Supreme Court has narrowed the scope of section 2511(1)(c) in one very particular set of circumstances. *Bartnicki v. Vopper*, 532 U.S. 514 (2001). In *Bartnicki*, several news organizations received a tape recording of a telephone conversation that they should have known was illegally intercepted. The majority held that the First Amendment prevents application of the statute to a disclosure of information of public concern by a third party not involved in the interception. The case involved a question of immunity from statutorily imposed civil liability, but the same First Amendment principles should apply to criminal liability as well.

Although *Bartnicki* demonstrates that the First Amendment does limit the applicability of section 2511(1)(c), the concurring opinions suggest that those limits are very narrow. For instance, a defendant will not be exempt from prosecution merely because he discloses information of interest to the public. Two of the six Justices in the majority in *Bartnicki* filed a separate concurring opinion that makes clear that a majority of the Court rejects a "public interest" exception to the disclosure provisions of the Wiretap Act. *See Bartnicki*, 532 U.S. at 540 (Breyer, J., concurring).

In concurring with the result in *Bartnicki*, Justice Breyer, with whom Justice O'Connor joined, agreed that privacy interests protected by section 2511(1)(c) must be balanced against media freedom embodied in the First Amendment. Justice Breyer wrote separately, however, to emphasize several facts he found particularly relevant in the case presented. In particular, he found that "the speakers had little or no *legitimate* interest in maintaining the privacy of the particular conversation." *Id.* at 539 (emphasis in original). Justice Breyer based this conclusion on three factors: (1) the content of the communication, (2) the public status of the speaker, and (3) the method by which the communication was transmitted. According to Justice Breyer, the conversation intercepted involved threats to harm others, which the law has traditionally treated as not entitled to remain private. Moreover, Justice Breyer concluded that the speakers were "limited public figures." *Id.* Finally, the speakers chose to communicate in what Justice Breyer viewed as an insecure method, via an unencrypted cellular

telephone. "Eavesdropping on ordinary cellular phone conversations in the street (which many callers seem to tolerate) is a very different matter from eavesdropping on encrypted cellular phone conversations or those carried on in the bedroom." *Id.* at 541.

Although prosecutors should be aware of the First Amendment limits outlined in *Bartnicki*, the First Amendment will probably be implicated very rarely. In *Bartnicki*, the Supreme Court explicitly did not address cases where (1) the disclosing party participated in any illegality in obtaining the information, or (2) the disclosure is of "trade secrets or domestic gossip or other information of purely private concern." *Id.* at 528, 533. In addition, the limits identified in *Bartnicki* explicitly do not apply to prosecutions under section 2511(1)(d) for using an illegally intercepted communication, which the Supreme Court expressly characterized as a regulation of conduct, not pure speech. *See id.* at 526-27.

Finally, note that the First Amendment does not create a general defense to Wiretap Act violations for media. If this was not obvious from the care with which the Supreme Court limited the exception in *Bartnicki*, several courts have explicitly so held. *See Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000); *Sussman v. ABC, Inc.*, 186 F.3d 1200 (9th Cir. 1999); *Vasquez-Santos v. El Mundo Broad. Corp.*, 219 F. Supp. 2d 221, 228 (D.P.R. 2002) (rejecting a blanket exemption from Wiretap Act liability for interceptions that occur for a tortious purpose during a media investigation).

C. Using an Intercepted Communication: 18 U.S.C. § 2511(1)(d)

Like a violation of subsection (1)(c), a charge under section 2511(1)(d) has three elements. The first two elements are the same as in section 2511(1)(c) and present the same issues discussed above.

Summary

1. Illegal interception of communication
2. knowledge or reason to know the intercept was illegal
3. use of the contents

Title 18, United States Code, Section 2511(1)(d) provides:

Except as otherwise specifically provided in this chapter any person who–

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that

the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection ….

shall be punished as provided in subsection (4).

The third element is different. "Use of the contents" of the intercepted communication is intended to be extremely broad. However, "use" does require some "active employment of the contents of the illegally intercepted communication for some purpose." *Peavy v. Harman*, 37 F. Supp. 2d 495, 513 (N.D. Tex. 1999), *aff'd in part and reversed in part*, 221 F.3d 258 (5th Cir. 2000). Accordingly, "use" does not include mere listening to intercepted conversations. *See, e.g., Dorris v. Absher*, 179 F.3d 420, 426 (6th Cir. 1999); *Reynolds v. Spears*, 93 F.3d 428, 432-33 (8th Cir. 1996); *Fields v. Atchison, Topeka and Santa Fe Ry. Co.*, 985 F. Supp. 1308 (D. Kan. 1997), *withdrawn in part*, 5 F. Supp. 2d (D. Kan 1998) ; *but see Thompson v. Dulaney*, 838 F. Supp. 1535, 1547 (D. Utah 1993) (finding listening was a use).

Because "use" is extremely broad, it may reach many of the cases that would otherwise be difficult to prosecute due to *Bartnicki*. For instance, a court has held that threatened disclosure in order to influence another is a "use." *See Leach v. Bryam*, 68 F. Supp. 2d 1072 (D. Minn. 1999). In the network context, other uses might include the use of intercepted passwords to gain access to other computers or use of intercepted confidential business information for commercial advantage.

D. Statutory Exceptions

The breadth of the Wiretap Act's general prohibitions against intercepting oral, wire, and electronic communications makes the statutory exceptions found in subsection 2511(2) particularly important. The exceptions that are particularly relevant in the context of network crimes are discussed below. A prosecutor should consider whether these exceptions apply in his or her case before undertaking a prosecution under the Wiretap Act. The applicability of these exceptions will be fact-dependent.

1. Provider Exception

The Wiretap Act provides that:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of a wire

> or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

18 U.S.C. § 2511(2)(a)(i).

The "rights or property of the provider" clause of subsection 2511(2)(a)(i) exempts providers from criminal liability for "intercept[ing] and monitor[ing communications] placed over their facilities in order to combat fraud and theft of service." *United States v. Villanueva*, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). For example, employees of a cellular phone company may intercept communications from an illegally "cloned" cell phone in the course of locating its source. *See United States v. Pervaz*, 118 F.3d 1, 5 (1st Cir. 1997). The rights or property clause also permits providers to monitor misuse of a system in order to protect the system from damage or invasions of privacy. For example, system administrators can track intruders within their networks in order to prevent further damage. *See United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (concluding that need to monitor misuse of computer system justified interception of electronic communications pursuant to subsection 2511(2)(a)(i)).

The rights and property clause of the provider exception does not permit providers to conduct unlimited monitoring. *See United States v. Auler*, 539 F.2d 642, 646 (7th Cir. 1976). The exception permits providers and their agents to conduct reasonable monitoring that balances the providers' need to protect their rights and property with their subscribers' right to privacy in their communications. *See United States v. Harvey*, 540 F.2d 1345, 1351 (8th Cir. 1976) ("The federal courts ... have construed the statute to impose a standard of reasonableness upon the investigating communication carrier.").

Thus, providers investigating unauthorized use of their systems have broad authority to monitor and disclose evidence of unauthorized use under subsection 2511(2)(a)(i), but should attempt to tailor their monitoring and disclosure to minimize the interception and disclosure of private communications unrelated

to the investigation. *See, e.g., United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975) (concluding that phone company investigating use of illegal devices designed to steal long-distance service acted permissibly under § 2511(2)(a)(i) when it intercepted the first two minutes of every illegal conversation but did not intercept legitimately authorized communications). In particular, there must be a "substantial nexus" between the monitoring and the threat to the provider's rights or property. *United States v. McLaren*, 957 F. Supp. 215, 219 (M.D. Fla. 1997); *see Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967) (interpreting Title III's predecessor statute, 47 U.S.C. § 605, and holding impermissible provider monitoring to convict blue box user of interstate transmission of wagering information).

Where a service provider supplies a communication to law enforcement that was intercepted pursuant to the rights and property exception, courts have scrutinized whether the service provider was acting as an agent of the government when intercepting communications. For example, in *McClelland v. McGrath*, 31 F. Supp. 2d 616 (N.D. Ill. 1998), a user of a cloned cellular telephone sued police officers for allegedly violating the Wiretap Act by asking telephone company to intercept his calls in connection with a kidnapping investigation. In dismissing the defendant's motion for summary judgment, the District Court found that a genuine issue of fact existed as to whether the phone company was impermissibly acting as the government's agent when it intercepted the plaintiff's call. *Id.* at 618. The Court opined that the officers were not free to ask or direct the service provider to intercept any phone calls or disclose their contents without complying with the judicial authorization provisions of the Wiretap Act, regardless of whether the service provider was entitled to intercept those calls on its own initiative. *Id.*; s*ee also United States v. McLaren*, 957 F. Supp. at 215. If the provider's interception of communications pursuant to the rights and property clause preceded law enforcement's involvement in the matter, no agency existed at the time of interception and the provider exception applies. *See United States v. Pervaz*, 118 F.3d at 5-6.

The "necessary … to the rendition of his service" clause of subsection 2511(2)(a)(i) permits providers to intercept, use, or disclose communications in the ordinary course of business when interception is unavoidable. *See United States v. New York Tel. Co.*, 434 U.S. 159, 168 n.13 (1977) (noting that § 2511(2)(a)(i) "excludes all normal telephone company business practices from the prohibition of [Title III]"). For example, a switchboard operator may briefly overhear conversations when connecting calls. *See, e.g., United States v. Savage*,

564 F.2d 728, 731-32 (5th Cir. 1977); *Adams v. Sumner*, 39 F.3d 933, 935 (9th Cir. 1994). Similarly, repairmen may overhear snippets of conversations when tapping phone lines in the course of repairs. *See United States v. Ross*, 713 F.2d 389, 392 (8th Cir. 1983). Although the "necessary incident to the rendition of his service" language has not been interpreted in the context of electronic communications, these cases concerning wire communications suggest that this phrase would likewise permit a system administrator to intercept communications in the course of repairing or maintaining a computer network.

For a more thorough discussion of this exception, see U.S. Department of Justice, *Searching and Seizing Computers and Electronic Evidence* (Office of Legal Education 2002), section IV.D.3.c.

2. Consent of a Party

The consent exceptions under paragraphs 2511(2)(c) and (d) are perhaps the most frequently cited exceptions to the Wiretap Act's general prohibition on intercepting communications. Section 2511(2)(c) provides:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or 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.

Under the Wiretap Act, government employees are not considered to be "acting under color of law" merely because they are government employees. *See Thomas v. Pearl*, 998 F.2d 447, 451 (7th Cir. 1993). Whether a government employee is acting under color of law under the wiretap statute depends on whether the individual was acting under the government's direction when conducting the interception. *See United States v. Andreas, 216 F.3d 645, 660 (7th Cir. 2000); United States v. Craig*, 573 F.2d 455, 476 (7th Cir, 1977); *see also Obron Atlantic Corp. v. Barr*, 990 F.2d 861, 864 (6th Cir. 1993); *United States v. Tousant*, 619 F.2d 810, 813 (9th Cir. 1980). The fact that a party to whom consent is provided is secretly cooperating with the government does not vitiate consent under paragraph 2511(2)(c). *United States v. Shields*, 675 F.2d 1152, 1156-57 (11th Cir. 1982).

The second exception provides that

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication

> where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d); *see also Payne v. Norwest Corp.*, 911 F. Supp. 1299, 1303 (D. Mont. 1995) (applying exception absent evidence of criminal or tortious purpose for recording of conversations), *rev'd on other grounds*, 113 F.3d 1079 (9th Cir. 1997). A criminal or tortious purpose must be a purpose other than merely to intercept the communication to which the individual is a party. *See Roberts v. Americable Int'l, Inc.*, 883 F. Supp. 499, 503 (E.D. Cal. 1995).

In the context of network communications, it may not always be clear who is a party to a communication capable of furnishing consent to intercept. The Senate report for the Wiretap Act defined "party" as "the person actually participating in the communication." S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182. Generally, a provider does not *participate* in the communications of its subscribers, but rather merely *transmits* them. Therefore, a service provider generally should not be considered a party to communications occurring on its system. Indeed, if service providers were capable of consenting to interception of communications as parties to communications occurring on their own systems, the exception that protects the rights and properties of service providers would be unnecessary. *See* 18 U.S.C. § 2511(2)(a)(i).

The courts have provided additional guidance about who constitutes a "party." It is clear, for example, that individuals are parties to a communication when statements are directed at them, even if they do not respond, *United States v. Pasha*, 332 F.2d 193 (7th Cir. 1964) (officer who answered phone during execution of warrant on gambling establishment was party to statements placing bets), or if they lie about their identity. *United States v. Campagnuolo*, 592 F.2d 852, 863 (5th Cir. 1979) (officer who answered phone in gambling establishment and pretended to be defendant was a party). At least one court appears to have taken a broader approach, holding that someone whose presence is known to other communicants may be a party, even if the communicants do not address her, nor she them. *See, e.g., United States v. Tzakis*, 736 F.2d 867, 871-72 (2d Cir. 1984). In appropriate cases, however, prosecutors should consider charging an individual who overhears or records conversations between

others who do not know that he is present, as such a person is not a party to the communication.

Consent under subsections 2511(2)(c) and (d) may be explicit or implied. *See United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987). The key to establishing implied consent in most cases is showing that the consenting party received actual notice of the monitoring and used the monitored system regardless. *See United States v. Workman*, 80 F.3d 688, 693 (2d Cir. 1996); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) ("[I]mplied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance.") (internal quotation marks omitted); *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998) ("Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception.") (internal quotation marks omitted). However, consent must be "actual" rather than "constructive." *See In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 19-20 (1st Cir. 2003) (*citing* cases). Proof of notice to the party generally supports the conclusion that the party knew of the monitoring. *See Workman*, 80 F.3d. at 693; *but see Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992) (finding lack of consent despite notice of possibility of monitoring). Absent proof of notice, it must be "convincingly" shown that the party knew about the interception based on surrounding circumstances in order to support a finding of implied consent. *See United States v. Lanoue*, 71 F.3d 966, 981 (1st Cir. 1995).

A network banner alerting the user that communications on the network are monitored and intercepted may be used to demonstrate that a user furnished consent to intercept communications on that network. *United States v. Angevine*, 281 F.3d 1130, 1133 (10th Cir. 2002); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

3. Computer Trespasser Exception

Section 2511(2)(i) allows victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Section 2511(2)(i) provides:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

Under paragraph 2511(2)(i), law enforcement—or a private party acting at the direction of law enforcement—may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, the four requirements found in section 2511(2)(i)(I)-(IV) must be met. Interceptions conducted by private parties not acting in concert with law enforcement are not permitted under the computer trespasser exception.

Under the definition of "computer trespasser" found in section 2510(21)(A), a trespasser includes any person who accesses a protected computer (as defined in 18 U.S.C. § 1030) without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the computer." 18 U.S.C. § 2510(21)(B). This provision, while harmless, was unnecessary, since a contractual relationship is just one way to show authority to access a network. For example, certain Internet service providers do not allow their customers to send bulk unsolicited emails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers—both because their access of the network is authorized and because they have an existing contractual relationship with the provider.

E. Defenses

In addition to the statutory exceptions provided by section 2511, section 2520 (which generally deals with recovery of civil damages) also includes several defenses against any civil *or criminal* action brought under the Wiretap Act. The "good faith" defenses in section 2520 prevent prosecution of a defendant who relied in good faith on listed types of lawful process (e.g., warrants, court orders, grand jury subpoenas) or an emergency request (under 18 U.S.C. § 2518(7)). 18 U.S.C. § 2520(d)(1), (2). These defenses are most commonly applicable to law enforcement officers executing legal process and service providers complying with legal process, even if the process later turns out to be deficient in some manner. Similarly, section 2520(d)(3) protects a person acting under color of law when that person believes in good faith that interception is warranted by the computer trespasser exception. *See* 18 U.S.C. § 2520(d)(3) (creating a defense for good faith reliance on a good faith determination that, *inter alia*, section 2511(2)(i) permitted the interception).

The final subsection of section 2520(d) provides that "good faith reliance" on "a good faith determination that section 2511(3) ... permitted the conduct complained of" is a "complete defense." 18 U.S.C. § 2520(d)(3). Section 2511(3) permits a provider of electronic communication service to the public to divulge the contents of communications under certain enumerated circumstances.

The defenses provided under subsection 2520(d) are affirmative defenses, *United States v. Councilman*, 418 F.3d 67, 89 (1st Cir. 2005), thus placing the burden of proof on the defendant. Whereas a mistake of law is not a defense for non-providers, *see* section B.1 of this chapter on page 64, some good faith mistakes of law are a defense for providers of electronic communication service to the public under subsection 2520(d)(3).

F. Statutory Penalties

A Wiretap Act violation is a Class D felony; the maximum authorized penalties for a violation of section 2511(1) of the Wiretap Act are imprisonment of not more than five years and a fine under Title 18. *See* 18 U.S.C. §§ 2511(4)(a) (setting penalties), 3559(a)(4) (classifying sentence). Authorized fines are typically not more than $250,000 for individuals or $500,000 for an organization, unless there is a substantial loss. *See* 18 U.S.C. § 3571 (setting fines for felonies). Generally applicable special assessments

and terms of supervised release also apply. *See* 18 U.S.C. § 3013(a)(2) (setting special assessments for felonies at $100 for individuals; $400 for persons other than individuals), 18 U.S.C. § 3583(b)(2) (allowing imposition of a term of supervised release not more than three years for a Class D felony).

For a discussion of the Sentencing Guidelines applicable to Wiretap Act violations, please see Chapter 5.

Chapter 3
Other Network Crime Statutes

A. Unlawful Access to Stored Communications: 18 U.S.C. § 2701

Section 2701 focuses on protecting email and voicemail from unauthorized access. *See* H.R. Rep. No. 647, 99th Cong., 2d Sess., at 63 (1986). At heart, section 2701 is designed to protect the confidentiality, integrity, and availability of such communications stored by providers of electronic communication service pending the messages' ultimate delivery to their intended recipients.

Summary

1. Intentional access
2. without or in excess of authorization
3. a facility that provided an electronic communication service
4. obtained, altered, or prevented authorized access to a communication in electronic storage
5. (felonies only) for commercial advantage, malicious destruction or damage, private commercial gain, or in furtherance of a criminal or tortious act

A charge under section 2701 has four essential elements. A felony conviction requires proof of one additional element.

Title 18, United States Code, Section 2701(a) provides:

Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

1. Intentional Access

The *mens rea* element of a section 2701 violation is that the defendant's unauthorized access (or access in excess of authorization) was intentional. Although no court has analyzed the *mens rea* requirement for this section,

courts have addressed the *mens rea* requirement for similar language in 18 U.S.C. § 1030. *See United States v. Sablan*, 92 F.3d 865, 867-68 (9th Cir. 1996); *United States v. Morris*, 928 F.2d 504, 508-09 (2d Cir. 1991). *Sablan* analyzed the wording, structure, and purpose of what was then § 1030(a)(5)(A) and concluded that the "intentionally" language modified only the "accesses without authorization" portion of that statute. *Sablan*, 92 F.3d at 868. The same reasoning applies to section 2701. Therefore, the government must prove that a defendant's access without authorization (or access in excess of authorization) was intentional.

The term "access" is not defined in this statute, but the term is discussed beginning on page 32. In a typical criminal case, in which a defendant will have logged on to a system and obtained, altered, or deleted email or voicemail, there will be no question that the defendant has accessed a facility.

2. Without or In Excess of Authorization

The second element of section 2701 requires proof that the defendant either was not authorized to access the facility or the defendant exceeded authorized access. This element mirrors the "without authorization" and "exceeds authorized access" language of 18 U.S.C. § 1030. For the discussion of the meaning of these terms, please see page 4.

3. Facility Through Which an Electronic Communication Service Is Provided

The third element of a section 2701 violation is that the defendant accessed a facility through which an electronic communication service (ECS) was provided. An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). In other words, an ECS is a facility that others use to transmit communications to third parties. Section 2701 incorporates that definition. *See* 18 U.S.C. § 2711(1). For example, logging on to an email server will satisfy this element. "[T]elephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568. A provider of email accounts over the Internet is a provider of ECS, *see FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 560 (N.D. Cal. 2000), as is the host of an electronic bulletin board. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879-80 (9th Cir. 2002). Thus, computers which provide such services are facilities through which an ECS is provided. *See Snow v. DirectTV*, 450 F.3d 1314 (11th Cir.

2006) (upholding a dismissal for failure to state a claim, where defendants used computers to access a website generally available to the public).

However, not every computer or device connected to a communication system is a facility through which an ECS is provided: a computer or device belonging to an end-user of ECS is not such a facility. For example, the Eleventh Circuit has held that hacking into a home computer does not by itself implicate section 2701, because a home computer does not provide an ECS to others. *See United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003). Similarly, the court in *State Wide Photocopy Corp. v. Tokai Fin. Services, Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995), rejected the assertion that a business's computers and fax machines constituted facilities through which an ECS is provided. Courts have also rejected the notion that maintaining a website or merely utilizing Internet access constitutes providing an ECS. *See Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196, 1999 (D.N.D. 2004) (holding that airline selling travel services over the Internet is not a provider of ECS); *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (holding that Amazon.com is not a provider of ECS).

4. Affected Authorized Access to a Communication In Electronic Storage

The fourth element of a section 2701 violation is that the defendant obtained, altered, or prevented authorized access to a wire or electronic communication while it was in "electronic storage." This element has three components. The first component, that the defendant "obtained, altered, or prevented authorized access to," means that a defendant must acquire a stored communication, modify a stored communication, or prevent proper access to a stored communication.

The Ninth Circuit, when distinguishing access under section 2701 from an interception under the Wiretap Act, misinterpreted this component. In *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998), the Ninth Circuit stated that "[t]he word 'intercept' entails *actually* acquiring the contents of a communication, whereas the word 'access' merely involves *being in position* to acquire the contents of a communication." *Smith*, 155 F.3d at 1058 (emphasis in original). It then opined that one might violate section 2701 by using a purloined password to log on to a voicemail system without ever obtaining the contents of any voicemail. *See id.*

This voicemail comment and definition of "access" ("obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage") indicate that the Ninth Circuit misread this component. It read "obtained," "altered," or "prevented authorized" as modifying "access to a wire or electronic communication," rather than reading "obtained," "altered," or "prevented authorized access to" as modifying "a wire or electronic communication." Thus, in the Ninth Circuit's voicemail example, the defendant will have obtained access to a wire communication, because the defendant will have been in a position to access the wire communication. However, even with the Ninth Circuit's definition of "access," this parsing of section 2701 does not make sense. In particular, it does not make sense for "altered" to modify "access to a wire or electronic communication." Instead, "altered" properly modifies "communication" and simply means "changed the communication." Because *Smith* misread section 2701, its definition of "access" should carry little weight.

The second component, that the conduct involved a "wire or electronic communication," needs little further explanation. Essentially, a wire communication is defined as a communication containing the human voice that is transmitted in part by wire or other similar method. *See* 18 U.S.C. § 2510(1), (18). In addition, "electronic communication" is defined broadly in 18 U.S.C. § 2510(12) and includes most electric or electronic signals that are not wire communications. For example, voicemail is a wire communication, and email and other typical Internet communications that do not contain the human voice are electronic communications.

The final component of this element is that the communication was in "electronic storage." The term "electronic storage" has a narrow, statutorily defined meaning. It does *not* simply mean storage of information by electronic means. Instead, "electronic storage" is "(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." 18 U.S.C. § 2510(17). As traditionally understood by the government, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of electronic communications service, and to backups of such intermediate communications. If the communication has been received by a recipient's service provider but has not yet been accessed by the recipient, it is in "electronic storage." For example, a copy of an email

or voicemail is in "electronic storage" only if it is at an intermediate point in its transmission and has not yet been retrieved by its intended recipient (e.g. "unopened email"). When the recipient retrieves the email or 18 U.S.C. §, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the communication on the service provider's system, the retained copy is no longer in "electronic storage" because it is no longer in "temporary, intermediate storage ... incidental to ... electronic transmission," and neither is it a backup of such a communication. *See Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001), *aff'd in part* 352 F.3d 107, 114 (3d Cir. 2004) (upholding district court's ruling on other grounds). Instead, it is treated like any other material stored by a user under provisions governing remote computing services. *See* H.R. Rep. No. 647, 99th Cong., 2d Sess., at 65 (1986) (stating that when a recipient has retrieved an email message and chooses to leave it in storage with the service provider, the email is protected under a provision of 18 U.S.C. § 2702 applicable to remote computing services).

This long-standing narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004). In *Theofel*, the Ninth Circuit held that email messages were in electronic storage regardless of whether they had been previously accessed. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that previously accessed email fell within the scope of the "backup" portion of the definition of "electronic storage." *See id.* at 1075. Under *Theofel*, essentially all stored wire or electronic communications are in "electronic storage."

If *Theofel*'s broad interpretation of "electronic storage" were correct, prosecutions under section 2701 would be substantially less difficult, as it can be hard to prove that communications fall within the traditional narrow interpretation of "electronic storage." However, CCIPS continues to question whether *Theofel* was correctly decided, since little reason exists for treating old email differently than other material a user may choose to store on a network. Any prosecutor considering a prosecution under section 2701 that relies on *Theofel* is urged to contact CCIPS for consultation.

5. Purpose

Felony charges require proof of one additional element: that the defendant acted "for purposes of commercial advantage, malicious destruction or damage,

or private commercial gain, or in furtherance of any criminal or tortious act." 18 U.S.C. § 2701(b)(1).[1] This element was added by the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), and it applies to conduct after January 23, 2003. All first-time violations of section 2701 prior to that date are misdemeanors. Such language is also used in the Wiretap Act, as an exception to when a party may consent to interception of their communications. *See* 18 U.S.C. § 2511(2)(d). In the Wiretap Act context, one appellate court has stated that this language is operative when a prohibited purpose is either the subject's primary motivation or a determinative factor in the subject's motivation. *See United States v. Cassiere*, 4 F.3d 1006, 1021 (1st Cir. 1993). Naturally, the "in furtherance of any criminal or tortious act" language means an act other than the unlawful access to stored communications itself. *See Boddie v. American Broadcasting Co.*, 731 F.2d 333, 339 (6th Cir. 1984).

6. Exceptions

Section 2701(c) provides three statutory exceptions to a violation. First, the section does not apply to "the person or entity providing a wire or electronic communication service." 18 U.S.C. § 2701(c)(1). Thus, unlike in the Wiretap Act context, service providers cannot violate § 2701, regardless of their motives in accessing stored communications. *See United States v. Councilman*, 418 F.3d 67, 81-82 (1st Cir. 2004) (en banc). Second, the section does not apply to conduct authorized by a user "with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002) (interpreting "user" narrowly to exclude someone who was properly authorized to access an electronic bulletin board, but who had not actually done so). Third, section 2701 does not apply to conduct authorized by other sections of the Act or the Wiretap Act. *See* 18 U.S.C. § 2701(c)(3). Although no court has yet addressed the role of these exceptions in a criminal prosecution, they should be viewed as creating affirmative defenses rather than statutory elements. *See generally United States v. Kloess*, 251 F.3d 941, 944-46 (11th Cir. 2001) (discussing distinctions between elements of a crime and affirmative defenses created by statutory exceptions).

[1] Similar language appears in the CFAA, 18 U.S.C. § 1030(c)(2)(B), to enhance the penalty for a violation of § 1030(a)(2), which criminalizes accessing a computer without authorization or in excess of authorization.

7. Penalties

The penalties for unlawful access to stored communications are divided into three categories. For first-time violations not committed for a specified improper purpose (that is, not committed "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act"), the maximum penalty is one year imprisonment and a $100,000 fine. *See* 18 U.S.C. §§ 2701(b)(2)(A), 3571(b)(5). For repeat violations not committed for an improper purpose, or for first-time violations committed for an improper purpose, the maximum penalty is five years' imprisonment and a $250,000 fine. *See* 18 U.S.C. §§ 2701(b)(1)(A), (b)(2)(B), 3571(b)(3). For repeat violations committed for an improper purpose, the maximum penalty is ten years' imprisonment and a $250,000 fine. *See* 18 U.S.C. §§ 2701(b)(1)(B), 3571(b)(3).

8. Historical Notes

The Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712, sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers. This system has three main substantive components that serve to protect and regulate the privacy interests of network users with respect to the world at large, network service providers, and the government. The first component of this system is a criminal prohibition. Under section 2701 of the SCA, anyone who obtains, alters, or prevents authorized access to certain stored communications is subject to criminal penalties. Neither of the other substantive components of the SCA is criminal: section 2702 regulates voluntary disclosure by network service providers of customer communications and records, and section 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications and related records.

Since its enactment in 1986, there have been very few prosecutions under section 2701. There are at least three reasons for this lack. First, prior to the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), all first-time violations of this section were misdemeanors. That Act, however, changed the maximum penalty for first-time violations to five years when the offense is committed "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State." 18 U.S.C. § 2701(b)(1). Second, one element of

prosecutions can be difficult to prove: that the defendant obtained, altered, or prevented authorized access to communications in "electronic storage," a term which is narrowly defined in 18 U.S.C. § 2510(17) and which has traditionally been interpreted to include only communications which have not yet been accessed by their intended recipient. Third, many violations of section 2701 also involve conduct that violates 18 U.S.C. § 1030. Because prosecutions under section 1030 do not involve proof that a communication is in "electronic storage," it will often be easier for the government to prove a violation of section 1030 than section 2701.

B. Identity Theft: 18 U.S.C. § 1028(a)(7)

Network intrusions can compromise the privacy of individuals if data about them or their transactions resides on the victim network. These cases should also be analyzed for potential violations of identity theft statutes. For a more detailed treatment of identity theft, see U.S. Department of Justice, *Identity Theft and Social Security Fraud* (Office of Legal Education 2004).

Several federal laws apply to identity theft, including 18 U.S.C. section 1028. That section criminalizes eight types of conduct involving fraudulent identification documents or the unlawful use of identification information. Section 1028(a)(7), enacted as part of the Identity Theft and Assumption Deterrence Act of 1998, and amended in 2004 by the Identity Theft Penalty Enhancement Act, will apply to some network crime cases.

Title 18, United States Code, Section 1028(a)(7) provides:

> *Whoever, in a circumstance described in subsection (c) of this section–*
>
> *(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable*
>
> *shall be punished as provided in subsection (b) of this section.*

The term "means of identification" is defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." 18 U.S.C. § 1028(d)(7). It covers several specific examples, such as name, social security number, date of birth, government issued driver's license and other numbers; unique biometric data, such as fingerprints, voice print, retina or iris image, or other unique physical

representation; unique electronic identification number, address, or routing code; and telecommunication identifying information or access device. *Id.*

Section 1028(a)(7) requires a predicate offense, much like 18 U.S.C. § 1028A (discussed below). Unlike section 1028A, however, the scope of section 1028(a)(7) is much broader. Section 1028A depends solely on certain enumerated federal felonies. *See* 18 U.S.C. § 1028A(a)(1). Section 1028(a)(7), on the other hand, may be based on *any* federal violation (felony or misdemeanor), as well as any local or state felony. *See* 18 U.S.C. § 1028(a)(7).

C. Aggravated Identity Theft: 18 U.S.C. § 1028A

The Identity Theft Penalty Enhancement Act, which took effect July 15, 2004, established a new offense of aggravated identity theft. Section 1028A adds an additional two-year term of imprisonment in cases where a defendant "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" during and in relation to any felony violation of certain enumerated federal offenses, including 18 U.S.C. §§ 1028 (but not 1028(a)(7)), 1029, 1030, 1037, and 1343. *See* 18 U.S.C. § 1028A(a)(1). In cases of terrorism-related aggravated identity theft, including that related to section 1030(a)(1), that section imposes an additional five-year term of imprisonment. 18 U.S.C. § 1028A(a)(2). In most cases, the additional terms of imprisonment will run consecutively, not concurrently. 18 U.S.C. § 1028A(b).

For questions regarding the application of this provision, please contact the Fraud Section of the Criminal Division of the Department of Justice at (202) 514-7023.

D. Access Device Fraud: 18 U.S.C. § 1029

Ten separate activities relating to access devices are criminalized in 18 U.S.C. § 1029. The term "access device" is broadly defined to mean "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."

18 U.S.C. § 1029(e)(1). Access devices related to network crimes might include passwords, electronic banking account numbers, and credit card numbers.

Generally speaking, section 1029 prohibits the production, use, possession, or trafficking of unauthorized or counterfeit access devices. Prosecutors should note the difference between "unauthorized" and "counterfeit" devices because certain key sections of the statute are based on these two terms. *See* 18 U.S.C. §§ 1029(e)(2) & (3). Section 1029 also covers activities related to certain tools and instruments that are used to obtain unauthorized use of telecommunications services. *See* 18 U.S.C. §§ 1029(a)(7)-(9).

Charges under section 1029 would be useful in many types of "phishing" cases, where a defendant uses fraudulent emails to obtain various types of passwords and account numbers, and "carding" cases, where a defendant purchases, sells, or transfers stolen bank account, credit card, or debit card information. Penalties for violations of section 1029 range from a maximum of 10 or 15 years' imprisonment depending on the subsection violated. *See* 18 U.S.C. § 1029(c)(1)(A). Second and later offenses are subject to 20 years' imprisonment. *See* 18 U.S.C. § 1029(c)(1)(B). Forfeiture is also available in many cases. *See* 18 U.S.C. §§ 1029(c)(1)(C), (c)(2).

For more information about section 1029, please contact the Fraud Section of the Criminal Division of the Department of Justice at (202) 514-7023. For specific information about subsections (7), (8), or (9), please contact CCIPS at (202) 514-1026.

E. CAN-SPAM Act: 18 U.S.C. § 1037

The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003), which became effective on January 1, 2004, provides a means for prosecuting those responsible for sending large amounts of unsolicited commercial email (a.k.a. "spam"). Although civil and regulatory provisions are the primary mechanism by which the CAN-SPAM Act's provisions are enforced, it also created several new criminal offenses at 18 U.S.C. § 1037. These offenses are intended to address more egregious violations of the CAN-SPAM Act, particularly where the perpetrator has taken significant steps to hide his or her identity, or the source of the spam, from recipients, ISPs, or law enforcement agencies.

In addition to section 1037, the CAN-SPAM Act contains another criminal provision, codified at 15 U.S.C. § 7704(d), which prohibits sending sexually explicit email that does not contain a label or marking designating it as sexually explicit. A knowing violation of this section is punishable by a fine, imprisonment for not more than five years, or both. For questions regarding the application of § 7704(d), please contact the Child Exploitation and Obscenity Section of the Criminal Division of the Department of Justice at (202) 514-5780.

Title 18, United States Code, Section 1037(a) provides:

Whoever, in or affecting interstate or foreign commerce, knowingly–

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b).

1. Commercial Electronic Mail Messages

Section 1037 only criminalizes conduct involving "commercial electronic mail messages":

> (A) In general. The term "commercial electronic mail message" means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial

product or service (including content on an Internet website operated for a commercial purpose).

(B) Transactional or relationship messages. The term "commercial electronic mail message" does not include a transactional or relationship message.

15 U.S.C. § 7702(2).

2. Materially

Sections 1037(a)(3) and (a)(4) require proof that certain information was "materially" falsified:

> For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

18 U.S.C. § 1037(d)(2).

3. Multiple

Section 1037 only criminalizes conduct involving "multiple" commercial email messages:

> The term "multiple" means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a one-year period.

18 U.S.C. § 1037(d)(3).

4. Penalties

A violation of section 1037 is a felony punishable by a fine, imprisonment for not more than five years, or both, if:

> (A) committed in furtherance of any felony under the laws of the U.S. or of any State; or

(B) the defendant has previously been convicted under § 1037, § 1030, or the law of any State for conduct involving the transmission of spam or unauthorized access to a computer system.

18 U.S.C. § 1037(b)(1).

A violation of section 1037 is a felony punishable by a fine, imprisonment for not more than three years, or both, if:

- committed in violation of § 1037(a)(1)
- committed in violation of § 1037(a)(4), and it involved 20 or more falsely registered email accounts, or 10 or more falsely registered domains
- the volume of email messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any one-year period
- the offense caused an aggregate loss of $5,000 or more to one or more persons during any one-year period
- any individual committing the offense obtained anything of value aggregating $5,000 or more during any one-year period; or
- the defendant undertook the offense with three or more persons and occupied an organizer or leadership position

18 U.S.C. § 1037(b)(2)(A)-(F).

All other violations of section 1037 are misdemeanors, punishable by a fine, imprisonment for not more than one year, or both. 18 U.S.C. § 1037(b)(3).

Section 1037 also contains specific provisions relating to forfeiture. 18 U.S.C. § 1037(c). For more information about forfeitures, please contact the Asset Forfeiture and Money Laundering Section of the Criminal Division of the Department of Justice at (202) 514-1263.

F. Wire Fraud: 18 U.S.C. § 1343

One particularly powerful and commonly applicable charge to consider is wire fraud. 18 U.S.C. § 1343. The United States Attorneys' Manual provides extensive guidance regarding wire fraud charges, *see* USAM § 9-43.000, as does the manual *Identity Theft and Social Security Fraud* (2004).

Title 18, United States Code, Section 1343 provides:

> *Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits, or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.*

1. Application to network crimes

Courts have recognized a variety of means of communications as falling under the wire fraud statute, including facsimile, telex, modem, and Internet transmissions. *See, e.g., United States v. Pirello*, 255 F.3d 728 (9th Cir. 2001) (affirming sentence of defendant who used the Internet to commit wire fraud).

Sections 1343 and 1030(a)(4) overlap to a degree in that both require fraudulent intent. Section 1343, however, carries significantly higher penalties. *Compare* 18 U.S.C. § 1343 (20 years' imprisonment; 30 years' imprisonment for fraud affecting financial institutions) *with* 18 U.S.C. § 1030(c)(3) (5 years' imprisonment for initial § 1030(a)(4) violation; 10 years for later violations). Section 1343 is also a predicate for RICO and money laundering charges, unlike section 1030 (with the exception of terrorism related violations of § 1030(a)(1) and 1030(a)(5)(A)(i)). For the full list of RICO predicate offenses, see 18 U.S.C. § 1961.

2. Penalties

Violations of this section are felonies, punishable by a fine, imprisonment for not more than 20 years, or both. 18 U.S.C. § 1343. If the violation affects a financial institution, the maximum penalty rises to a fine of up to $1,000,000, imprisonment for not more than 30 years, or both. *Id.*

G. Communication Interference: 18 U.S.C. § 1362

Where a compromised computer is owned or used by the United States for communications purposes, 18 U.S.C. § 1362 may provide an alternative or additional charge.

Title 18, United States Code, Section 1362 provides:

> *Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both.*

1. Application to Network Crimes

Section 1362 applies to "any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States." 18 U.S.C. § 1362. The list of covered communications systems could include, for example, those used to provide electronic mail services.

Section 1362 is particularly useful in cases where the intrusion into a U.S. Government system would be a misdemeanor under § 1030 (e.g., first time violations of § 1030(a)(2)(B), (a)(3), (a)(5)(A)(iii), or (a)(6)(B)), but could be charged as a ten-year felony under § 1362.

2. Penalties

A violation of this section is a felony punishable by a fine, imprisonment for not more than 10 years, or both. 18 U.S.C. § 1362.

Chapter 4
Special Considerations

A. Jurisdiction

1. Interstate Commerce or Communication Requirement

Several of the statutes discussed in this manual require an interstate or foreign jurisdictional hook. *See, e.g.,* 18 U.S.C. § 1029(a) (prohibiting access device fraud "if the offense affects interstate or foreign commerce"); 18 U.S.C. § 2510(12) (defining "electronic communication" to mean any "transfer of signs, signals, writing, images, sounds, data, or intelligence ... that affects interstate or foreign commerce"). Failure to establish the "interstate" basis for federal jurisdiction can lead to dismissal or acquittal. *See United States v. Jones*, 580 F.2d 219 (6th Cir. 1978) (affirming judgment of acquittal in wiretap case where government failed to offer evidence that telephone company provided facilities for the transmission of interstate or foreign communications).

Many of the charges in 18 U.S.C. § 1030 prohibit unlawful access of a "protected computer," which includes a computer used in "interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). In most cases, demonstrating that a computer was connected to the Internet will satisfy this requirement. Section 1030(a)(2)(C) requires a more particular nexus—the unlawful conduct itself must involve an interstate or foreign communication. *See* 18 U.S.C. § 1030(a)(2)(C). Prosecutors should be prepared to offer evidence that the conduct in fact traversed state lines. Useful evidence might include testimony as to the geographic location of computer servers. Bear in mind that even a "local" provider may utilize communication facilities in another state.

2. Extraterritoriality

Absent evidence of a contrary intent, the laws of the United States are presumed *not* to have extraterritorial application. *See United States v. Cotten*, 471 F.2d 744, 750 (9th Cir. 1973). This presumption against extraterritoriality may be overcome by showing "clear evidence of congressional intent to apply a statute beyond our borders." *United States v. Gatlin*, 216 F.3d 207, 211 (2d Cir. 2000) (internal quotations omitted). "Congress has the authority to enforce its

laws beyond the territorial boundaries of the United States. Whether Congress has in fact exercised that authority in [a particular case] is a matter of statutory construction." *Equal Employment Opportunity Comm. v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991) (internal citations omitted).

In 2001, as part of the USA PATRIOT Act, Congress revised both sections 1029 and 1030 to explicitly provide for extraterritorial jurisdiction in certain cases. The USA PATRIOT Act added the following language to section 1029:

> (h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—
>
> > (1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and
> >
> > (2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

18 U.S.C. § 1029(h).

The Act also amended section 1030(e)(2)(B) to specifically include a computer "which is used in interstate or foreign commerce, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *See* 18 U.S.C. § 1030(e)(2)(B). Even prior to the 2001 amendment, however, at least one court held that the plain language of 18 U.S.C. § 1030 was a clear manifestation of congressional intent to apply that section extraterritorially. *See United States v. Ivanov*, 175 F. Supp. 2d 367, 374-75 (D. Conn. 2001).

Extraterritorial jurisdiction can be found not only on the basis of specific congressional intent, but also on the basis of intended and actual detrimental effects within the United States. "The intent to cause effects within the United States ... makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope." *United States v. Muench*, 694

F.2d 28, 33 (2d Cir. 1982). "It has long been a commonplace of criminal liability that a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which that evil is the fruit." *United States v. Steinberg*, 62 F.2d 77, 78 (2d Cir. 1932).

Other sources of extraterritorial jurisdiction may include 18 U.S.C. § 7, which defines the special maritime and territorial jurisdiction of the United States, and 18 U.S.C. §§ 3261-3267, which govern criminal offenses committed outside of the United States by members of the military and persons employed by or accompanying them.

B. Venue

1. Background

Venue is governed by a combination of constitutional provisions, statutes, and rules. *See* 2 Charles Alan Wright, *Federal Practice & Procedure* § 301 (3d ed. 2000). The Constitution mandates that trial be held in the state and district where the crime was committed. *See* U.S. Const. art. III, § 2, cl. 3; U.S. Const. amend. VI. This principle is implemented by Federal Rule of Criminal Procedure 18, which states in full: "Unless a statute or these rules permit otherwise, the government must prosecute an offense in a district where the offense was committed. The court must set the place of trial within the district with due regard for the convenience of the defendant and the witnesses, and the prompt administration of justice." Fed. R. Crim. P. 18. However, the Constitution and Rule 18 still leave many questions unanswered in many network crime cases, such as how to define where an offense has been "committed" or how to deal with crimes committed in multiple states or countries.

Note that when a defendant is charged with more than one count, venue must be proper with respect to each count. *See United States v. Salinas*, 373 F.3d 161, 164 (1st Cir. 2004) ("The criminal law does not recognize the concept of supplemental venue"). If no single district has proper venue for all potential counts, prosecutors can either charge the defendant in multiple districts and seek transfer to a single district or bring all charges in one district and seek a waiver from the defendant. Rule 20 of the Federal Rules of Criminal Procedure allows transfer of prosecution for purposes of entering a guilty plea, from the district where the indictment is pending to the district where the defendant is arrested, held, or present. Similarly, Rule 21 allows a court to transfer a prosecution for trial, upon the defendant's motion, to another district for the

convenience of the parties and witnesses. Note, however, that both rules require the explicit consent and cooperation of the defendant. A defendant may also waive any objections to improper venue, either explicitly or by failing to object when the defect in venue is clear. *See United States v. Roberts*, 308 F.3d 1147, 1151-52 (11th Cir. 2002); *United States v. Novak*, 443 F.3d 150, 161 (2d Cir. 2006).

2. Locations of Network Crimes

Applying the principles of venue to network crimes is not always a straightforward endeavor. As described above, the central inquiry in venue analysis is determining where the crime was committed. Yet, "in today's wired world of telecommunication and technology, it is often difficult to determine exactly where a crime was committed, since different elements may be widely scattered in both time and space, and those elements may not coincide with the accused's actual presence." *United States v. Saavedra*, 223 F.3d 85, 86 (2d Cir. 2000); *see United States v. Rowe*, 414 F.3d 271 (2d Cir. 2005) (finding venue in district where agent connected to Internet, entered chat room, and saw defendant's posting in child porn case).

None of the intrusion crimes discussed in Chapter 1 contains specific venue provisions. Moreover, few reported cases address venue for these crimes. *See, e.g., United States v. Ryan*, 894 F.2d 355 (10th Cir. 2000) (noting that 18 U.S.C. § 1029 does not specify venue); *Berger v. King World Productions, Inc.*, 732 F. Supp. 766 (E.D. Mich. 1990) (examining venue under 28 U.S.C. § 1391(b) in a civil suit arising pursuant to 18 U.S.C. § 2511).

Multidistrict offenses "may be ... prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a) Note that only the "essential conduct elements" of a crime qualify. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280 (1999). For instance, section 1030(a)(2)(C) prohibits intentionally accessing a computer without or in excess of authorization, and thereby obtaining information from any protected computer if the conduct involved an interstate or foreign communication. The two essential conduct elements in section 1030(a)(2)(C) are "accessing" a computer and "obtaining" information. Thus, it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access *and* where the information is obtained.

The exact location of each event—the "accessing" and the "obtaining"—may not always be easily determined.

Example: *An intruder located in California uses communications that pass through a router in Arizona to break into a network in Illinois, and then uses those network connections to obtain information from a server in Kentucky.*

The intruder initiated access in California, the router in Arizona enabled that access, but arguably the intruder did not achieve access until reaching the network in Illinois. Of course, one could also argue that access did not occur until the intruder reached the server in Kentucky where the information was located. Likewise, the intruder may have obtained the information in Kentucky, or he may not have obtained the information until it reached him in the district where he was located, in this case, California.

This example illustrates an offense governed by 18 U.S.C. § 3237(a). Under any of the options discussed above, the appropriate venue would seem to include both of the endpoints—that is, the district in which the offender is located (California) and the district in which the information is located (Kentucky). It is likely that venue is also proper at some, if not all, of the points in between, since venue may lie "in any district in which [a continuing] offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Under this section, the "accessing" and "obtaining" were arguably continued in Arizona and Illinois. Certainly, venue seems proper in Illinois where the intruder broke into the network. Whether it can be said that the intruder committed a crime in Arizona is less clear.

Prosecutors looking to fix venue in the locale where communications simply pass through, as in the case of the router in Arizona, should look closely at the facts to determine whether venue in that district would satisfy the framework discussed above.[1] The case for "pass through" venue may be stronger where transmission of the communications themselves constitutes the criminal offense (e.g., when a threatening email is sent in violation of 18 U.S.C. § 1030(a)(7)) and the path of transmission is certain (e.g., when an AOL subscriber's email is sent through a mail server in Virginia).[2] By contrast, in cases where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because packets of information

[1] As a practical matter, it may be difficult to prove that the intruder's communications traveled through a particular router in a particular geographic location.

[2] The type of "pass through" venue described in this paragraph does not cover the situation where the "pass through" computer itself is hacked. In that case, venue would likely be proper based on the hack rather than the "pass through."

happened to travel through that district. *Cf. Ashcroft v. ACLU*, 535 U.S. 564, 602 (2002) (Kennedy, J., concurring) ("In the context of COPA, it seems likely that venue would be proper where the material originates or where it is viewed. Whether it may be said that a website moves "through" other venues in between is less certain.").

Federal prosecutors should also take note of the Department of Justice's policies for wire and mail fraud, which may be analogous. For wire fraud, section 967 of the Department's Criminal Resource Manual provides that prosecutions "may be instituted in any district in which an interstate or foreign transmission was issued or terminated." *Crim. Resource Manual* § 967. Although the text of section 967 refers only to the place of issuance or termination, the case cited in support of that proposition, *United States v. Goldberg*, 830 F.2d 459, 465 (3d Cir. 1987), relies on 18 U.S.C. § 3237(a), which also includes the place where the conduct continued, thus leaving open the door to "pass through" venue. In the case of mail fraud, section 9-43.300 of the U.S. Attorneys' Manual "opposes mail fraud venue based solely on the mail matter passing through a jurisdiction." USAM 9-43.300; see also Crim. Resource Manual § 966.

In some cases, venue might also lie in the district where the effects of the crime are felt. The Supreme Court has not faced that question directly. *See United States v. Rodriguez-Moreno*, 526 U.S. 275, 279 n.2 (1999) ("The Government argues that venue also may permissibly be based upon the effects of a defendant's conduct in a district other than the one in which the defendant performs the acts constituting the offense. Because this case only concerns the *locus delicti*, we express no opinion as to whether the Government's assertion is correct."). However, other courts that have examined the issue have concluded that venue may lie "where the effects of the defendant's conduct are felt, but only when Congress has defined the essential conduct elements in terms of those effects." *United States v. Bowens*, 224 F.3d 302, 314 (4th Cir. 2000), *cert. denied,* 532 U.S. 944 (2001). Thus, charges under provisions like 18 U.S.C. § 1030(a)(5) may be brought where the effects are felt because those charges are defined in terms of "damage," even if the bulk of network crimes may not be prosecuted in a district simply because the effects of the crime are felt there. Prosecutors seeking to establish venue by this method are encouraged to contact CCIPS at (202) 514-1026.

C. Statute of Limitations

With one exception, the Computer Fraud and Abuse Act subsections discussed in Chapter 1 do not contain a specific statute of limitations for criminal prosecutions. *But see* 18 U.S.C. § 1030(g) (requiring *civil* actions to be brought "within 2 years of the date of the act complained of or the date of the discovery of the damage"); 18 U.S.C. § 2707(f) (creating two-year statute of limitations for *civil* actions); 18 U.S.C. § 2520(e) (providing that any *civil* action "may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation").

In the absence of a specific statute of limitations, the default federal limitations period of five years applies. *See* 18 U.S.C. § 3282. The exception to the five-year default limit is 18 U.S.C. § 1030(a)(1), which is now included in the list of offenses in 18 U.S.C. § 2332b(g)(5)(B), which offenses are incorporated into 18 U.S.C. § 3286. The statute of limitation for those crimes is extended to eight years, and is totally eliminated for offenses that resulted in, or created a foreseeable risk of, death or serious bodily injury to another person.

For cases involving evidence located in a foreign country, prosecutors can request that the court before which an investigative grand jury is impaneled suspend the statute of limitations, if the court finds by a preponderance of the evidence: (1) that an official request has been made for such evidence; and (2) that it reasonably appears, or reasonably appeared at the time the request was made, that such evidence is, or was, in such foreign country. *See* 18 U.S.C. § 3292. Note that such requests may be made *ex parte*, must be made before return of an indictment, and must bear sufficient indicia of reliability, such as by sworn or verified application. *See United States v. Trainor*, 376 F.3d 1325 (11th Cir. 2004).

D. Juveniles[3]

In the 1983 movie *War Games*, Matthew Broderick and Ally Sheedy play high school students who inadvertently access the NORAD computer network, thinking that they are merely playing a "war game" with the computers. As

[3] This section is adapted from an article written by Joseph V. DeMarco, Assistant United States Attorney for the Southern District of New York, and published in the May 2001 U.S. Attorneys' Bulletin. Mr. DeMarco currently serves as a Computer Hacking and Intellectual Property Coordinator in the Southern District and formerly served as a detailee to CCIPS.

a consequence, Broderick and Sheedy come Hollywood-close to initiating a nuclear exchange between the United States and the Soviet Union. In order to accomplish this hack, Broderick configures his computer's modem to automatically dial random telephone numbers in the city where the computers he hopes to break into are located. When Sheedy asks Broderick how he pays for all the telephone calls, Broderick coyly tells her that "there are ways around" paying for the phone service. Sheedy asks: "Isn't that a crime?" Broderick replies: "Not if you are under eighteen."

This section demonstrates why Broderick was wrong. Federal prosecutors can bring juvenile offenders to justice, but must understand the applicable provisions of the criminal code. Specifically, the Federal Juvenile Delinquency Act (FJDA), 18 U.S.C. §§ 5031-5042, governs the criminal prosecution and the delinquent adjudication of minors in federal court.

While a complete analysis of the FJDA is beyond the scope of this manual, certain of its provisions merit discussion because proceedings against juveniles in federal court differ in significant respects from the prosecution of adults. The FJDA creates a unique procedure for delinquency proceedings against juveniles—a process that is quasi-criminal and quasi-civil in nature, replete with its own procedural complexities and particular rules.

As a threshold matter, it is important to note that a juvenile proceeding is not the same as a criminal prosecution. Rather, it is a proceeding in which the issue to be determined is whether the minor is a "juvenile delinquent" as a matter of status, not whether he or she is guilty of committing a crime. Thus, a finding against the juvenile does not result in a criminal conviction; instead, it results in a finding of "delinquency." Indeed, the juvenile proceeding is specifically designed to *lessen* the amount of stigma that attaches to the act of delinquency compared to a criminal conviction, and to emphasize the rehabilitation, rather than punishment, of the juvenile. *See, e.g., United States v. Hill*, 538 F.2d 1072, 1074 (4th Cir. 1976). With that background in mind, several aspects of the FJDA are examined below.

1. Definition of Juvenile

Under the FJDA, a "juvenile" is a person who has not yet reached the age of eighteen at the time of the commission of the offense *and* is under twenty-one as of the time of the filing of formal juvenile charges. *See* 18 U.S.C. § 5031. Thus, a person who committed the offense before his eighteenth birthday, but is over twenty-one on the date formal charges are filed, may be prosecuted as

an adult. The juvenile delinquency proceedings would not apply at all in that case. This is true even where the government could have charged the juvenile prior to his twenty-first birthday, but did not. *See In re Jack Glenn Martin*, 788 F.2d 696, 698 (11th Cir. 1986) (holding that determinative date is date of filing of formal indictment or information; fact that government could have brought charges against defendant prior to his twenty-first birthday held to be "irrelevant"); *see also United States v. Hoo*, 825 F.2d 667 (2d Cir. 1987) (holding that absent improper delay by government, age at time of filing of formal charges determines whether FJDA applies).

2. Federal Jurisdiction

As is true in the case of adults, not every criminal act committed by a juvenile violates federal law. Only where Congress has determined that a particular federal interest is at stake, and has passed appropriate legislation, can a federal criminal prosecution go forward. In general, under the FJDA, there are three situations where federal delinquency jurisdiction over a juvenile exists. The first is where the state court lacks jurisdiction or refuses to assume jurisdiction. *See* 18 U.S.C. § 5032. The second is where the state does not have available programs and services adequate for the needs of juveniles. *See id.* The third is where the crime is a federal felony crime of violence or one of several enumerated federal offenses (principally relating to narcotics and firearm offenses), and a substantial federal interest exists to warrant exercise of federal jurisdiction. *See id.*

No State Statute or State Refuses Jurisdiction

This first basis for federal jurisdiction will be the most frequently used basis in the context of juvenile delinquency involving computers. It encompasses situations where a state has no law criminalizing the specific conduct, or does have a law, but for whatever reason, indicates that it will not pursue proceedings under its law against the minor. With regard to the former, although many states have enacted laws analogous to statutes such as the federal network crime statute (18 U.S.C. § 1030), the electronic wiretap statute (18 U.S.C. § 2511), and the access device fraud statute (18 U.S.C. § 1029), some states do not have laws under which the acts in question can be prosecuted. In these cases, the FJDA nevertheless allows the juvenile to be held accountable for his or her act of delinquency under federal law.

More commonly, however, a state will have a statute that does cover the crime in question, *see, e.g.,* N.Y. Penal Law § 156.10 (computer trespass);

§ 156.27 (computer tampering in the first degree); § 250.05 (intercepting or accessing electronic communications), but will be unwilling to assume jurisdiction over the juvenile, perhaps because of a shortage of resources, or a dearth of technical or prosecutorial expertise. In such cases, upon certification by the United States Attorney that pertinent state officials do not wish to proceed against the juvenile, the federal government may assume jurisdiction. *See* 18 U.S.C. § 5032.

In the context of intrusion crimes, certain offenses committed by juveniles may amount to crimes in multiple states. A crippling denial of service attack or the transmission of a computer virus can generate victims in numerous jurisdictions. The FJDA, however, does not appear to require the government to certify that each and every state that could potentially assert jurisdiction is unwilling to assume that jurisdiction. The FJDA merely requires that the "juvenile court or other appropriate court of *a State* does not have jurisdiction or refuses to assume jurisdiction over [the] juvenile." 18 U.S.C. § 5032 (emphasis added). Typically, the pertinent state will be the state contemplating proceedings against the minor which, in practice, will often be the state in which the federal prosecutor investigating the case sits. Of course, because federal criminal proceedings can often preclude state criminal proceedings under state double jeopardy principles, federal prosecutors faced with multistate cases should consult with prosecutors from all affected states in order to determine what, if any, effect a federal juvenile proceeding may have on a state's proceedings. Consultation is also warranted because certain states may provide for treatment of the juvenile as an adult more easily than the transfer provisions of the FJDA (discussed below).

The State Has No Programs or Inadequate Programs

This second basis for federal jurisdiction arises infrequently, as most states do in fact have programs and facilities that provide for the adjudication, detention, and rehabilitation of minors. However, in the event that state officials were, for any reason, unable to address the needs of a juvenile, this exception would apply.

Enumerated Crimes and Crimes of Violence

The FJDA sets forth certain federal crimes for which jurisdiction is deemed to exist where there is a substantial federal interest. The enumerated offenses are controlled substance offenses under 21 U.S.C. §§ 841, 952(a), 953, 955, 959, 960(b)(1), (2), or (3), as well as firearms-related offenses under 18 U.S.C.

§§ 922(x), 924(b), (g), or (h). While these offenses typically do not apply to computer intrusion cases, the FJDA also permits jurisdiction in cases of "crimes of violence" that are punishable as felonies. *See* 18 U.S.C. § 5032. Although the FJDA itself does not define "crimes of violence," 18 U.S.C. § 16 states that such offenses "ha[ve] as an element the use, attempted use, or threatened use of physical force against the person or property of another." 18 U.S.C. § 16. "Crimes of violence" also include any offense "that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense." 18 U.S.C. § 16.

Most of the intrusion offenses discussed in this manual do not involve physical force. However, several statutes may implicate this basis for jurisdiction in the context of computer-related crime, including 18 U.S.C. § 875(b) (transmission in interstate or foreign commerce of extortionate threats to injure another person), 18 U.S.C. § 1951(a) and (b)(2) (interference with commerce by extortion or threats of physical violence), and 18 U.S.C. § 844(e) (transmission of bomb threats).

Prosecutors relying on this third basis for jurisdiction should keep in mind that their certification must not only set forth a federal felony crime of violence, but must also certify that a substantial federal interest in the case or offense justifies federal jurisdiction. Eight of the nine circuits that have addressed the issue have held that the United States Attorney's certification of a substantial federal interest is not subject to appellate review for factual accuracy; only the Fourth Circuit has held otherwise. *See United States v. John Doe*, 226 F.3d 672, 676-78 (6th Cir. 2000) (collecting cases).

Where the federal government is the victim of a crime, the federal interest is apparent. Yet, even when the government is not the victim, federal interests often exist because network crimes affect critical infrastructures (e.g., telecommunications systems), industries or technologies significant to the nation's economy (e.g., aerospace, computer software), or are committed by criminals operating in multiple states and/or foreign countries. In these important and hard-to-enforce-locally situations, federal jurisdiction may be particularly appropriate.

3. Delinquency Proceedings

Assuming that federal juvenile jurisdiction exists, prosecutors bringing such actions will typically commence the action with the filing, under seal,

of a juvenile information and the jurisdictional certification. *See* 18 U.S.C. § 5032. It is important to note that the certification must be signed by the United States Attorney personally, and a copy of the pertinent memorandum delegating authority from the Assistant Attorney General to the United States Attorney to sign the certification should be attached to the submission. *See id.* (requiring certification of "the Attorney General").

A juvenile has no Fifth Amendment right to have his or her case presented to a grand jury, nor does the juvenile have the right to a trial by jury. *See, e.g., United States v. Hill*, 538 F.2d 1072, 1075-76 (4th Cir. 1976); *United States v. Indian Boy*, 565 F.2d 585, 595 (9th Cir. 1975). Instead, the "guilt" phase of a delinquency proceeding is essentially conducted as a bench trial. In that trial, the government must prove that the juvenile has committed the act of delinquency beyond a reasonable doubt, and the juvenile has many of the same rights as a criminal defendant. These include: (1) the right to notice of the charges; (2) the right to counsel; (3) the right to confront and cross-examine witnesses; and (4) the privilege against self-incrimination. *See Hill*, 538 F.2d at 1075 n.3 (collecting cases). Moreover, in the delinquency proceeding, the Federal Rules of Criminal Procedure apply to the extent that their application is not inconsistent with any provision of the FJDA. *See* Fed. R. Crim. P. 1(a)(5)(D); *see also* 3B Charles Alan Wright et al., *Federal Practice & Procedure* § 873 (3d ed. 2004). The Federal Rules of Evidence likewise apply to the delinquency proceeding, *see* F.R.E. 101, 1101, although courts have held them inapplicable to transfer proceedings (discussed below). *See Government of the Virgin Islands in the Interest of A.M., a Minor*, 34 F.3d 153, 160-62 (3d Cir. 1994) (collecting cases).

The Act also affords juveniles special protections not ordinarily applicable to adult defendants. Most notably, the juvenile's identity is protected from public disclosure. *See* 18 U.S.C. § 5038 (provisions concerning sealing and safeguarding of records generated and maintained in juvenile proceedings). Thus, court filings should refer to the juvenile by his or her initials and not by name, and routine booking photographs and fingerprints should not be made or kept. Moreover, when a juvenile is taken into custody for an alleged act of delinquency, the juvenile must be informed of his or her legal rights "in language comprehensible to [the] juvenile," 18 U.S.C. § 5033, and the juvenile's parent, guardian, or custodian must be notified immediately of the juvenile's arrest, the nature of the charges, and the juvenile's rights. *Id.* Upon arrest, the juvenile may not be detained for longer than a reasonable period

of time before being brought before a magistrate. *Id.* When brought before a magistrate, the juvenile must be released to his or her parents or guardian upon their promise to bring the juvenile to court for future appearances, unless the magistrate determines that the detention of the juvenile is required to secure his or her appearance before the court, or to insure the juvenile's safety or the safety of others. *See* 18 U.S.C. § 5034. At no time may a juvenile who is under twenty-one years of age and charged with an act of delinquency or adjudicated delinquent be housed in a facility where he or she would have regular contact with incarcerated adults. *See* 18 U.S.C. §§ 5035, 5039. Under the FJDA, a juvenile has a right to counsel at all critical stages of the proceeding, and the FJDA authorizes the appointment of counsel where the juvenile's parents or guardian cannot afford to retain counsel. *See* 18 U.S.C. § 5034.

4. Transfers to Adult Criminal Proceedings

As noted above, under certain circumstances, a juvenile's case may be transferred to adult status and the juvenile can be tried as an adult. In these situations, the case proceeds as any criminal case would, with the exception that a juvenile under eighteen who is transferred to adult status may *not* be housed with adults at any time pretrial or post trial. *See* 18 U.S.C. §§ 5035, 5039. A juvenile may transfer to adult status by waiving his juvenile status, upon written request and advice of counsel. *See* 18 U.S.C. § 5032. In addition, the FJDA creates two forms of transfer which do not depend on waiver: discretionary transfer and mandatory transfer.

As the name implies, discretionary transfer is an option available, upon motion by the government, in certain types of cases where the juvenile is fifteen or older at the time of the commission of the act of delinquency. *See* 18 U.S.C. § 5032. Such transfer is available in cases involving felony crimes of violence and other enumerated crimes. Under the FJDA, a court must consider six factors in determining whether it is in the interest of justice to grant the government's motion for discretionary transfer: (1) the age and social background of the juvenile; (2) the nature of the alleged offense, including the juvenile's leadership role in a criminal organization; (3) the nature and extent of the juvenile's prior delinquency record; (4) the juvenile's present intellectual development and psychological maturity; (5) the juvenile's response to past treatment efforts and the nature of those efforts; and (6) the availability of programs to treat the juvenile's behavioral problems. *See* 18 U.S.C. § 5032. In the context of typical computer crimes committed by juveniles, several of the factors will often counsel in favor of transfer to adult status: many computer

delinquents come from middle-class or affluent backgrounds; many commit their exploits with the assistance of other delinquents; and many are extremely intelligent. Moreover, many of the most sophisticated computer criminals are barely under the age of eighteen and, as such nearly-adult offenders, may merit punishment as adults.

Mandatory transfer is much more circumscribed than discretionary transfer; it is limited to either certain enumerated offenses (e.g., arson), which typically are not applicable in network crime prosecutions, or to violent felonies directed against other persons. *See* 18 U.S.C. § 5032. Mandatory transfer is also limited to offenses committed by juveniles sixteen or older who have a prior criminal conviction or juvenile delinquency adjudication for which they could be subject to mandatory or discretionary transfer. As a practical matter, therefore, in the area of network crimes, the majority of proceedings begun as juvenile proceedings will likely remain as such, and will not be transferred to adult prosecutions.

Federal prosecutors who are considering filing a motion to transfer a juvenile proceeding to adult criminal court should notify the Domestic Security Section of the Criminal Division at (202) 616-5731.

5. Sentencing and Detention

Under the FJDA, a court has several options in sentencing a juvenile adjudged to be delinquent. The court may suspend the finding of delinquency, order restitution, place the juvenile on probation, or order that the juvenile be detained. *See* 18 U.S.C. § 5037(a). In cases where detention is ordered, such detention can never be longer than the period of detention the juvenile would have received had he or she been an adult. *See* 18 U.S.C. § 5037(b). Accordingly, the Sentencing Guidelines, although not controlling, must be consulted. *See* U.S.S.G. § 1B1.12; *see also United States v. R.L.C.*, 503 U.S. 291, 307 n.7 (1992). Finally, if the disposition hearing is before the juvenile's eighteenth birthday, he or she may be committed to official detention until his or her twenty-first birthday or the length of time he or she would have received as an adult under the Sentencing Guidelines, whichever term is less. If the juvenile is between eighteen and twenty-one at the time of the disposition, he or she may be detained for a maximum term of three or five years (depending on the type of felony relevant to the proceeding), but in no event can he or she be detained longer than the comparable adult sentence under the Guidelines. *See* 18 U.S.C. § 5037(b), (c).

6. Other Considerations

As demonstrated above, federal delinquency proceedings are unique from a legal point of view, and prosecutors initiating such proceedings would do well to consult closely with the provisions of the United States Attorneys' Manual concerning delinquency proceedings, *see* USAM § 9-8.00, as well as the Domestic Security Section, which serves as the Department's expert in this field. Prosecutors should also familiarize themselves with the legal issues typically litigated in this area in order to avoid common pitfalls. *See, e.g.*, Jean M. Radler, Annotation, *Treatment Under Federal Juvenile Delinquency Act (18 U.S.C. §§ 5031-5042) of Juvenile Alleged to Have Violated Law of United States*, 137 A.L.R. Fed. 481 (1997).

In addition to the novel nature of the proceedings themselves, crimes committed by juveniles pose unique investigative challenges. For example, common investigative techniques such as undercover operations and the use of cooperators and informants can raise difficult issues rarely present in the investigation of adults. Indeed, a seemingly routine post-arrest interview may raise special issues of consent and voluntariness when the arrestee is a juvenile. *Compare United States v. John Doe*, 226 F.3d 672 (6th Cir. 2000) (affirming district court's refusal to suppress juvenile's confession notwithstanding arresting officer's failure to comply with parental notification provisions of FJDA, where circumstances surrounding the confession demonstrated voluntariness of juvenile's confession) *with United States v. Juvenile (RRA-A)*, 229 F.3d 737 (9th Cir. 2000) (ruling that juvenile's confession should be suppressed where arresting officer's failure to inform parents may have been a factor in confession, notwithstanding juvenile's request to arresting officers that her parents *not* be contacted and informed of the arrest).

Consider also the case of a juvenile in a foreign country who uses the Internet to damage a government computer or an e-commerce web server. Ordinarily, extradition of foreign nationals to the United States is governed by treaty. Some extradition treaties contain provisions that specifically permit the foreign sovereign to take account of the youth of the offender in deciding whether to extradite. *See, e.g.*, Convention on Extradition Between the United States and Sweden, 14 U.S.T. 1845; T.I.A.S. 5496 (as supplemented by Supplementary Convention on Extradition, T.I.A.S. 10812). Other treaties are silent on the issue of juveniles. How these situations will unfold in the future is unclear. Prosecutors who encounter situations involving network crimes by juveniles operating from abroad, should, in addition to consulting with Domestic

Security Section, consult with the Department's Office of International Affairs at (202) 514-0000.

Chapter 5
Sentencing

This section addresses the United States Sentencing Guidelines ("Guidelines"), as well as the specific offense characteristics and adjustments, most commonly applicable to network crimes. This chapter should be read in light of the Supreme Court decision in *United States v. Booker*, 543 U.S. 220 (2005), which holds that courts must consider the United States Sentencing Guidelines but that the Guidelines are advisory rather than mandatory.

The Guidelines treat most network crimes as basic economic offenses for which U.S.S.G. § 2B1.1 determines an offender's sentence. This guideline applies to property damage, theft, and fraud. Wiretap violations are sentenced under a different Guideline, U.S.S.G. § 2H3.1, which is discussed in Section C, below.

A. Base Offense Levels

Table 4 sets forth the applicable offense conduct guideline and base offense level for each of the crimes discussed in this manual. When the conviction is for an attempted violation of 18 U.S.C. § 1030(b), courts should apply the appropriate guideline for the substantive offense and then decrease the offense level by three. *See* U.S.S.G. § 2X1.1(a), (b)(1).

Table 4. Sentencing Guidelines for Network Crimes

Section of 18 U.S.C.	Guidelines	Base Offense Level
§ 1028(a)(7) § 1029 § 1030(a)(2), (4), (5), (6) § 1037 § 1343 § 1362 § 2701	§ 2B1.1	6; 7 if the statutory maximum term for defendant's conviction is 20 years or more
§ 1030(a)(1)	§ 2M3.2	30; 35 for TS information
§ 1030(a)(3)	§ 2B2.3	4
§ 1030(a)(7)	§ 2B3.2	18
§ 2511	§§ 2B5.3, 2H3.1	8, 9

As noted in Table 4, most network crimes will be sentenced under U.S.S.G. § 2B1.1. An offense sentenced under this section is usually assigned a basic offense level of 6.

B. Adjustments Under Section 2B1.1

After determining the base offense level, prosecutors must determine whether any specific offense characteristics and adjustments may apply. Several relevant specific offense characteristics and adjustments are discussed below.

1. Loss

Under U.S.S.G. § 2B1.1(b)(1), the base offense level is increased based on how much monetary loss the defendant caused according to a loss table:

TABLE 5. GUIDELINES ADJUSTMENTS FOR LOSS

Loss	Increase
$5,000 or less	0
More than $5,000	2
More than $10,000	4
More than $30,000	6
More than $70,000	8
More than $120,000	10
More than $200,000	12
More than $400,000	14

Loss	Increase
More than $1,000,000	16
More than $2,500,000	18
More than $7,000,000	20
More than $20,000,000	22
More than $50,000,000	24
More than $100,000,000	26
More than $200,000,000	28
More than $400,000,000	30

The government bears the burden of proving the amount of loss by a preponderance of the evidence. *See United States v. Jackson*, 155 F.3d 942, 948 (8th Cir. 1998). Courts are not required to determine precisely the amount of loss attributable to a defendant. Rather, "[t]he court need only make a reasonable estimate of the loss." U.S.S.G. § 2B1.1, cmt. n.3(C); *see also Elliott v. United States*, 332 F.3d 753, 766 (4th Cir. 2003); *Jackson*, 155 F.3d at 948. That reasonable estimate should take into account available information, including, but not limited to, the following: "[t]he fair market value of the property taken ... and revenues generated by similar operations." U.S.S.G. § 2B1.1 cmt. n.3(C)(i), (v).

In estimating the loss resulting from a defendant's unlawful intrusions, courts should include the reasonable cost of any harms caused by his criminal conduct. Such amounts should include the reasonable value of the property taken by defendant (such as the data copied). Moreover, the Application Notes instruct the court to use the greater of actual loss or intended loss to determine the appropriate offense level increase for an offender. U.S.S.G. § 2B1.1, cmt. n.3(A). If there is no reliable means of determining loss, the court is directed to use the gain to the defendant instead. U.S.S.G. § 2B1.1, cmt. n.3(B); *cf.*

United States v. Chatterji, 46 F.3d 1336, 1340 (4th Cir. 1995) (holding that gain cannot be used where there is no loss); *United States v. Andersen*, 45 F.3d 217, 221-22 (7th Cir. 1995) (same).

Generally, "actual loss" is limited to "reasonably foreseeable pecuniary harm that resulted from the offense." In addition, the definition of "intended loss" makes it clear that intended pecuniary harm should be counted even if it "would have been impossible or unlikely to occur." (See the discussion of the "economic realities" doctrine on page 114).

Beyond the general rules for calculating loss under the Guidelines, there is an additional comment that expands the definition of "actual loss" to include certain additional harms, whether or not reasonably foreseeable, in cases brought under 18 U.S.C. § 1030. U.S.S.G. § 2B1.1, cmt. n.3(A)(v)(III). The commentary to the 2005 Guidelines states that for such offenses:

> actual loss *includes* the following pecuniary harm, *regardless of whether such pecuniary harm was reasonably foreseeable:* any reasonable cost to the victim including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.

Id. (emphasis added).

Note that this definition adds to the normal definition of "actual loss" used to calculate sentences under the Guidelines. Accordingly, it is not to be used in place of, but rather in addition to, the fair market value of the data taken by a defendant. This additional language expands the usual definition of "actual loss" for section 1030 offenses by including the value of certain pecuniary harms even if not reasonably foreseeable. However, this expansion only applies to "actual loss" and not to "intended loss." *Id*.

In a recent case, the Eighth Circuit upheld a sentence where the District Court calculated loss using the value of specialty commercial software illegally copied by the defendant. The Court of Appeals upheld the District Court's decision to rely upon the testimony of software professionals who estimated the loss using development costs and data from a recent transaction involving that software. *United States v. Ameri*, 412 F.3d 893, 900-01 (8th Cir. 2005).

At least one Circuit has also allowed costs reasonably associated with "preventing further damage resulting from Defendant's conduct." *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000). Such costs must not be "excessive" and may not be costs that "merely create an improved computer system unrelated to preventing further damage." ***Id.*** Given that instructions for exploiting known computer network vulnerabilities are easily shared via the Internet, the cost incurred by a victim to prevent attacks of those who might follow the defendant may be allowable as well.

With the exception of offenses under 18 U.S.C. § 1030(a)(5) and civil suits brought under 18 U.S.C. § 1030(g), loss is not an element of any offense under § 1030. While there is very little published case law on the subject of calculating loss for sentencing purposes under § 1030(a)(5), there are a number of cases that address the issue of loss in civil suits authorized under 18 U.S.C. § 1030(g). Section 1030(g) requires that civil plaintiffs prove one of the factors in 1030(a)(5)(B)—typically loss of more than $5,000—before they can prevail. ("Loss" is discussed in detail beginning on page 37).

With respect to sentencing in criminal cases brought under section 1030, however, loss is a central question. Furthermore, there are parallels between the language in the Guideline commentary for loss in section 1030 cases and the definition of loss that is a required element to prove a violation under 18 U.S.C. § 1030(a)(5), and, therefore, to support a civil claim under 18 U.S.C. § 1030(g). Compare 18 U.S.C. § 1030(e)(11) with U.S.S.G. § 2B1.1, cmt. n.3(A)(v)(III). Section 1030(e)(11) begins the definition of "loss" by stating that loss "means any reasonable cost to any victim." It then goes on to provide a nonexclusive list of costs that may be included within the definition of "loss" such as:

> the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service ….

18 U.S.C. § 1030(e)(11). This list is substantially similar to the list in the Guidelines commentary for § 2B1.1. *See* U.S.S.G. § 2B1.1, cmt. n.3(A)(v)(III). However, as was discussed previously, the commentary in the Guidelines merely provides authority to expand the normal definition of "actual loss" for such offenses and is not a substitute for the value of the property unlawfully taken by a defendant.

In contrast, for civil cases brought under 18 U.S.C. § 1030(g), loss is limited to the definition set forth in section 1030(e)(11). In that context, a number of courts have held that revenue lost because a computer system was down due to an intrusion would be "loss," but revenue lost to competitors who used customer data stolen from the victim would not. *See Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 381 (S.D.N.Y. 2005) (holding "that revenue lost because a defendant used unlawfully gained information to unfairly compete was not a type of 'loss' contemplated under the CFAA") (citing *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 478 (S.D.N.Y. 2004)). According to this line of civil cases, lost revenue (e.g., from lost goodwill or lost business opportunities) would only be "loss" under the 1030(e)(11) "if it resulted from the impairment or unavailability of data or systems." *Nexans*, 319 F. Supp. 2d 468, 477.

Although the concept of loss may be constrained in civil cases brought under section 1030(g)—or when establishing a criminal violation under section 1030(a)(5)—prosecutors should be prepared to explain that courts are not similarly constrained when calculating loss at the time of sentencing for section 1030 offenses. In a criminal sentencing for a "protected computer" offense, the loss that stems from the intrusion is merely one type of loss to be tallied. For example, the fair market value of the data copied unlawfully by a defendant is clearly a proper category of loss to be attributed to him at sentencing, regardless of whether or not that value could have been used to satisfy the loss requirement in section 1030(a)(5).

Where a network offense includes use of a victim's services without or in excess of authorization, loss may include the cost to the victim of providing such services. *Cf. America Online, Inc. v. National Health Care Discount, Inc.*, 174 F. Supp. 2d 890, 900-02 (N.D. Iowa 2001) (awarding AOL $0.78 per thousand pieces of electronic mail that a spammer caused to be delivered in violation of AOL's use policy). Loss does not include, however, expenses incurred cooperating with law enforcement's investigation of the offense. U.S.S.G. § 2B1.1, cmt. n.3(D)(ii); cf. *United States v. Sablan*, 92 F.3d 865, 870 (9th Cir. 1996) (excluding "expenses incurred due to meetings with the FBI" from loss calculation for purposes of restitution).

Finally, section 2B1.1 offers special instructions for determining loss in cases involving "unauthorized access devices." Section 2B1.1 adopts the definitions used in 18 U.S.C. § 1029 for the terms "counterfeit access device" and "unauthorized access device." *See* U.S.S.G. § 2B1.1, cmt. n.3(F)(i),

n.9(A). The statute's broad definition includes any code, account number, password, personal identification number, or other means of account access that has been stolen, forged, or obtained with intent to defraud. *See* 18 U.S.C. § 1029(e)(1)-(3); *United States v. Petersen*, 98 F.3d 502, 505 (9th Cir. 1996) (treating computer passwords as access devices). Where a defendant obtains access devices without authorization, by hacking a password file or by Internet credit card phishing, for example, "loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall not be less than $500 per access device." U.S.S.G. § 2B1.1, cmt. n.3(F)(i).

In a credit card phishing case in which the defendant charged $45,000 worth of purchases to fraudulently-obtained credit card numbers, possessed an additional 250 credit card numbers that he had not used, and also possessed 150 email account passwords, the loss would be equal to the sum of the charges ($45,000), $500 for each unused credit card number (250 x $500 = $125,000), and $500 for each password (150 x $500 = $75,000), a total loss of $245,000 and an offense level increase of 12. Remember that $500 per access device is the minimum loss; if the actual charges exceed $500, the higher figure should be used instead. Under certain circumstances, it may even be appropriate to determine intended loss by aggregating the credit limits of the access devices: "[W]here a sentencing court has facts upon which to base findings that a defendant was capable of and intended to use the [credit] cards to secure amounts at or near their credit limits, aggregating the credit limits of the cards to calculate loss is appropriate." *See United States v. Say*, 923 F. Supp. 611, 614 (D. Vt. 1995) (citing *United States v. Egemonye*, 62 F.3d 425 (1st Cir. 1995); *United States v. Sowels*, 998 F.2d 249 (5th Cir. 1993)).

2. Economic Realities Defense

The appropriate loss figure for calculating the guideline sentence under the applicable Guidelines is "the greater of actual or intended loss." U.S.S.G. § 2B1.1(b)(1), cmt. n.3(A). Some defendants may, however, attempt to cite *United States v. Stockheimer* for the proposition that disparity between the intended loss and the foreseeable, potential loss overstates the seriousness of the offense. *United States v. Stockheimer*, 157 F.3d 1082 (7th Cir. 1998). They may argue that this "economic realities" doctrine justifies either a reduction in the calculated loss or a downward departure.

However, the holdings in cases such as *Stockheimer* have effectively been rendered moot by amendments to the Guidelines. See *United States v. McBride*,

362 F.3d 360, 374 (6th Cir. 2004) (holding "the amendments abandon this circuit's interpretation of intended loss") (citing *United States v. Anderson*, 353 F.3d 490, 505 n.13 (6th Cir. 2003)). Under the current Guidelines, the likelihood that a scheme might be incapable of yielding the entire amount of loss intended is no longer to be considered when calculating the guideline range. The general rule that the greater of intended or actual loss should be used is still valid. U.S.S.G. § 2B1.1(b)(1), cmt. n.3(A). Since Amendment 617 took effect on November 1, 2001, the term "intended loss" is defined to include "intended pecuniary harm that would have been impossible or unlikely to occur (e.g., as in a government sting operation, or an insurance fraud in which the claim exceeded the insured value.)." U.S.S.G. § 2B1.1(b)(1), cmt. n.3(A)(ii).

The "Reason for Amendment" commentary for Amendment 617 makes it clear that the purpose of the amendment was to address decisions such as *Stockbridge* where departures were granted based on the "economic realities" doctrine. "Concepts such as 'economic reality' or 'amounts put at risk' will no longer be considerations in the determination of intended loss." U.S.S.G. Amendment 617, November 1, 2001 (citing *United States v. Bonanno*, 146 F.3d 502 (7th Cir. 1998) (holding that the relevant inquiry is how much the scheme put at risk); *United States v. Wells*, 127 F. 3d 739 (8th Cir. 1997) (holding that intended loss properly was measured by the possible loss the defendant intended, and did not hinge on actual or net loss)).

In light of the language of Amendment 617 and the Application Notes in the commentary for § 2B1.1, it is clear that under the current Guidelines defendants are to be held responsible for all the loss they intend. The "economic reality" doctrine is no longer a consideration and should not serve as basis for either a reduction in the calculated loss or a downward departure under that theory. U.S.S.G. § 2B1.1(b)(1), cmt. n.2(A).

3. Number of Victims

Section 2B1.1 imposes a graduated increase in offense level based on the number of victims that suffered actual loss as a result of the offense. *See* U.S.S.G. § 2B1.1(b)(2), cmt. n.1. If the offense causes loss to ten or more victims, the offense level is increased by two; if it causes loss to fifty or more victims, the offense level is increased by four; and if it causes loss to 250 or more victims, the offense level is increased by six. This specific offense characteristic may be particularly important in network crimes such as the propagation of worms or viruses, crimes that, by their very nature, involve a large number of victims.

Although this specific offense characteristic takes into account only those victims that suffered actual loss as a result of the offense, courts have suggested that in cases in which there is a large, unrealized intended loss, an upward departure may be appropriate. *See United States v. Mohammed*, 315 F. Supp. 2d 354 (S.D.N.Y. 2003). Similarly, although the specific offense characteristic does not take into account victims that have suffered non-monetary harm, it may be appropriate for the court to depart upward if there are a large number of such victims. *See* U.S.S.G. § 2B1.1, cmt. n.19(A)(ii) (indicating that upward departure may be appropriate if "[t]he offense caused or risked substantial non-monetary harm").

4. Extraterritorial Conduct

The Guidelines indicate that the sentencing court should increase the base offense level by two or, if such an increase does not result in an offense level of at least twelve, to twelve if "a substantial part of a fraudulent scheme was committed from outside the United States." U.S.S.G. § 2B1.1(b)(9)(B). Although no reported case offers insight into how courts will apply this specific offense characteristic to network crimes that cross international boundaries, there is a strong argument to be made that, even if an offender is physically located within the United States, if he avails himself of a foreign email account to receive, possess, and distribute messages in furtherance of a fraudulent scheme, he is subject to a two-level increase provided for in this specific offense characteristic. Similarly, if an intruder avails himself of a computer in another country as a tool dump site or a zombie through which he can intrude into other computers or launch attacks, his conduct falls within the scope of this specific offense characteristic.

In *United States v. Singh*, 291 F.3d 756 (11th Cir. 2002), the defendant engaged in an elaborate scheme to obtain international long-distance telephone service free of charge for sale to third parties. After initiating a long-distance account with an American carrier using false information, the defendant would call his Kuwaiti "clients," who would then provide him a number (usually in a third country) with which they wished to be connected. The defendant would use the three-way calling feature of his phone service to connect the Kuwaiti client. The telephone companies were unable to charge defendant for these international calls (or anything else, for that matter) due to the fraudulent account information. Although the defendant did not originate this scheme outside the United States or personally take action outside the United States, and the government did not produce any evidence as to the identity or number

of his coconspirators in Kuwait, the court upheld a sentencing enhancement on the basis that a substantial portion of the scheme was committed from outside the United States.

5. Sophisticated Means

Section 2B1.1 advises sentencing courts to increase the offense level by two levels (or to increase the offense level to 12, if the two-level increase results in an offense level lower than 12) if "the offense ... involved sophisticated means." U.S.S.G. § 2B1.1(b)(9)(C). A "sophisticated means" enhancement is appropriate if the offense includes "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." U.S.S.G. § 2B1.1, cmt. n.8(B). The Application Note offers use of a fictitious business entity to perpetrate a fraud as an example of a "sophisticated means." See also *United States v. Paradies*, 98 F.3d 1266, 1292 (11th Cir. 1996).

There are few reported cases regarding the application of the sophisticated means enhancement to a computer crime defendant. *See, e.g., United States v. Harvey*, 413 F.3d 850 (8th Cir. 2005) (defendants' use of a computer to generate authentic looking checks as part of fraudulent scheme upheld as partial basis for sophisticated means enhancement); *United States v. O'Brien*, 435 F.3d 36 (1st Cir. 2006) (in section 1030(a)(5) case, upholding sentencing increase based on use of special skill—commission of the offense involved knowledge of specific computer program, which required special training, and defendant had considerable skill in using that program, as demonstrated by fact that he taught class for that program).

By analogy to other areas of criminal law, it seems likely that the enhancement would apply to an online fraud scheme involving a fictitious business entity or a network intrusion or assault directed through several compromised computers. Prosecutors contemplating application of this enhancement to a computer crime are encouraged to contact CCIPS.

6. Trafficking in Access Devices

Section 2B1.1 advises sentencing courts to increase the offense level by two levels (or to increase the offense level to 12, if the two-level increase results in an offense level lower than 12) if "the offense involved ... trafficking of any unauthorized access device or counterfeit access device." U.S.S.G. § 2B1.1(b)(10)(B). The definition of "access device" includes computer passwords and credit cards. *See* 18 U.S.C. § 1029(e)(1); *United States v. Peterson*,

98 F.3d 502, 505 (9th Cir. 1996) (acknowledging district court's treatment of computer passwords as "access devices"); *United States v. Caputo*, 808 F.2d 963, 966 (2d Cir. 1987) (upholding district court finding that restaurant receipts containing credit card numbers are access devices). This specific offense characteristic may therefore be applicable to computer intrusion cases in which the intruder obtained the victim's password and to online fraud cases in which the perpetrators obtain the victims' password, credit card number, social security number, or bank account information.

7. Risk of Death or Injury

As basic services such as medical treatment, emergency response, public transportation, water treatment, and military protection rely increasingly on computer networks for their maintenance and operation, the risk that a computer crime might cause death or serious bodily injury increases. Section 2B1.1 takes this into account, providing a two-level increase (or an increase to level 14, if the two-level increase results in an offense level less than 14) "[i]f the offense involved ... the conscious or reckless risk of death or serious bodily injury." U.S.S.G. § 2B1.1(b)(12)(A). To merit this enhancement, the government must demonstrate by a preponderance of the evidence that the defendant was aware that his conduct created a risk of death or serious bodily injury and that he nonetheless consciously or recklessly disregarded that risk. See *United States v. McCord, Inc.*, 143 F.3d 1095, 1098 (8th Cir. 1998). Courts have upheld application of this enhancement for a medical researcher who falsely reported the efficacy of a course of treatment for skin cancer, causing test subjects to forego other forms of treatment (see *United States v. Snyder*, 291 F.3d 1291, 1295 (11th Cir. 2002)), for a defense contractor who provided helicopter armor that had not undergone ballistics tests when the contract required pretested armor (see *United States v. Cannon*, 41 F.3d 1462, 1467 (11th Cir. 1995)), and for an airport security manager who consciously disregarded screening and testing requirements for airport security personnel (see *United States v. Saffer*, 118 F. Supp. 2d 546, 548-49 (E.D. Pa. 2000)).

8. Private Information

Effective November 1, 2003, a new specific offense characteristic took effect. The new provision covers a seemingly random collection of subjects, providing sentencing enhancements for each. A defendant either gets an enhancement for obtaining personal information or for intentionally causing damage or for substantially disrupting a critical infrastructure, but no two of

these enhancements may be combined to sentence an offense that, for instance, involves both intentionally damaging a computer and obtaining personal information. Below, each of these new enhancements will be addressed in turn.

The first enhancement directs a sentencing court to increase by two the offense level of any defendant convicted of violating 18 U.S.C. § 1030 if his offense involved "an intent to obtain personal information." U.S.S.G. 2B1.1(b)(14)(A)(i)(II).[1] An accompanying note, Application Note 13, defines personal information as:

> sensitive or private information (including such information in the possession of a third party), including (i) medical records; (ii) wills; (iii) diaries; (iv) private correspondence, including email; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.

Although the information obtained in many cases will fall squarely within the examples listed in this definition, other cases may require courts to extrapolate and determine whether specific information is of a kind that a reasonable computer user would consider sensitive or private.

Two aspects of this provision deserve brief discussion. First, the provision does not require a defendant to actually obtain personal information—he must merely intend to obtain it. So, for instance, a defendant who accessed without authorization an email service provider's mail server but was unable to gain access to subscribers' emails would receive this enhancement if the evidence also included an email or a chat session in which he indicated that his intent was to obtain subscribers' emails and mine them for sensitive, valuable information. Second, the provision uses the term "obtain," a term which has been used broadly in the online context to include accessing or merely observing information. *See* S. Rep. No. 99-432, at 6-7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 (noting that "'obtaining information' [for the purposes of 18 U.S.C. § 1030(a)(2)] includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.").

[1] Section 2B1.1 indicates that "a substantial invasion of a privacy interest" is one valid ground for an upward departure. U.S.S.G. § 2B1.1, cmt. n.19(A)(ii).

9. Intentional Damage

The second new enhancement, U.S.S.G. § 2B1.1(b)(14)(A)(ii), requires a sentencing court to increase a defendant's offense level by four if the defendant was convicted of a violation of 18 U.S.C. § 1030(a)(5)(A)(i), which proscribes transmission of a program, information, code or command if such conduct intentionally causes unauthorized damage. This enhancement applies to any conviction under this statutory subsection, effectively raising the base offense level for such violations to 10.

10. Critical Infrastructures

The final new enhancement takes a "three-tiered" approach to computer crimes affecting or relating to "critical infrastructures." An Application Note defines "critical infrastructure" as:

> systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines and airports), and government operations that provide essential services to the public.

U.S.S.G. § 2B1.1, cmt. n.13(A).

The first tier directs a court to increase a defendant's offense level by two if the offense was a violation of 18 U.S.C. § 1030 that "involved ... a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security." U.S.S.G. § 2B1.1(b)(14)(A)(i). This lowest tier enhancement applies even if the computer in question is not damaged or disrupted; mere access to such a computer is sufficient to trigger the two-level increase.

The second tier imposes a six-level enhancement (or, if the resulting offense level is still less than 24, an increase to 24) for violations of § 1030 that "caused a substantial disruption of a critical infrastructure." U.S.S.G. § 2B1.1(b)(14)(A)(iii), (b)(14)(B).

The third tier indicates that an upward departure (beyond offense level 24) is appropriate if a violation of § 1030 is "so substantial as to have a *debilitating impact* on national security, *national* economic security, *national* public health or safety, or any combination of those matters." U.S.S.G. § 2B1.1, cmt. n.19(B) (emphasis added). The Sentencing Commission provides little guidance as to what qualifies as a "substantial disruption" or as a "debilitating impact." In defining "debilitating impact," the Commission added the word "national" as a modifier of "security," "economic security," and "public health or safety," indicating that with regard to these factors, a local (as opposed to national) disruption will not qualify as "debilitating."

C. CAN-SPAM Act

Section 2B1.1 contains a new two-level increase for defendants who are convicted of violating the CAN-SPAM Act, 18 U.S.C. § 1037, and whose offense "involved obtaining electronic mail addresses through improper means." U.S.S.G. § 2B1.1(b)(7). The commentary states that the term "improper means" includes "unauthorized harvesting of electronic mail addresses of users of a website, proprietary service, or other online public forum." U.S.S.G. § 2B1.1, cmt. n.6. Prosecutors considering use of this enhancement are encouraged to contact CCIPS.

In addition, under U.S.S.G. § 2B1.1(b)(2)(A)(ii), a violator of section 1037 will automatically receive at least a two-level increase for mass-marketing, and may receive a larger increase based on the number of victims.

D. Wiretap Act

Sentences for most violations of the Wiretap Act involving network crimes are addressed by Guideline § 2H3.1 (Interception of Communications; Eavesdropping; Disclosure of Tax Return Information).[2] The base offense level is nine. U.S.S.G. § 2H3.1(a)(1). If the purpose of the offense was to obtain commercial advantage or economic gain, the offense level increases by three. U.S.S.G. § 2H3.1(b). If the violation also constitutes an attempt to commit another offense, courts should apply the guideline that would result in a greater offense level. U.S.S.G. § 2H3.1(c)(1).

[2] Wiretap Act violations also may fall under Guideline § 2B5.3 (Criminal Infringement of Copyright or Trademark). As reflected in the Commentary, this provision is intended primarily for the interception of copyrighted satellite transmissions.

As a result of being grouped differently than most other network crimes, violations of the Wiretap Act generally begin with a higher Base Offense Level. This leads to a beginning sentencing range at least four months greater than comparable interceptions of stored communications. Compare U.S.S.G. § 2H3.1(a)(1) (base offense level 9 corresponding to imprisonment of 4-10 months at Criminal History Category I) with U.S.S.G. § 2B1.1(a)(2) (base offense level 6 corresponding to 0-6 months imprisonment at Criminal History Category I).

However, Wiretap Act violations are not subject to the same specific offense characteristics and adjustments available in Guideline § 2B1.1. The absence of these potential enhancements to the offense level for, among other things, the amount of loss caused by the offense, could result in much shorter sentences for Wiretap Act violations than for unauthorized access to stored communications.

For instance, a Wiretap Act violation not committed for economic gain by a person with no criminal history would result in a sentencing range of 4-10 months. Such a defendant would be in Zone B and thus eligible for a sentence of probation (combined with intermittent confinement, community confinement, or home detention). *See* U.S.S.G. § 2H3.1. The amount of loss caused by the individual's interception will not affect the sentence.

In contrast, an intruder who illegally accessed a stored communication in violation of 18 U.S.C. § 2701 (rather than intercepting a communication contemporaneous with its transmission) faces a sentence that is potentially much more severe. Under section 2701, a sentence can be heavily influenced by the amount of damage caused by the intruder conduct. For instance, if an intruder's conduct caused more than $1,000,000 in loss, that individual would face a minimum sentence of almost three and one-half years.

E. Generally-Applicable Adjustments

1. Overview

The sentencing adjustments set forth in Chapter 3 of the Guidelines may further alter the base offense level. In particular, if the computer crime involved or was intended to promote a federal crime of terrorism, U.S.S.G. § 3A1.4 may apply. It also may be appropriate to adjust the defendant's sentence based on his role in the crime. The defendant may have played an aggravating role (U.S.S.G.

§ 3B1.1) or a mitigating role (U.S.S.G. § 3B1.2), may have used special skill (U.S.S.G. § 3B1.3), or may have involved a minor in the commission of the crime (U.S.S.G. § 3B1.4). If the defendant has tried to delete or destroy evidence, or otherwise frustrate law enforcement's investigation of his crime, an obstruction adjustment may also be appropriate (U.S.S.G. § 3C1.1). On the other hand, if the defendant has been forthcoming about his role in committing the offense and has cooperated with law enforcement, a downward adjustment for acceptance of responsibility may be appropriate (U.S.S.G. § 3E1.1).

2. Special Skill

Section 3B1.3 of the Guidelines advises sentencing courts to increase a defendant's offense level by two "[i]f the defendant ... used a special skill[] in a manner that significantly facilitated the commission or concealment of the offense." Section 3B1.3 cautions, however, that courts should not impose the enhancement if the factual predicate that justifies a special skill enhancement has already been the basis for a specific offense characteristic (such as the "sophisticated means" characteristic under U.S.S.G. § 2B1.1). However, "so long as the court finds a sufficient independent factual basis for both" a sophisticated means enhancement and a special skill enhancement, "it may impose both." *United States v. Minneman*, 143 F.3d 274, 283 (7th Cir. 1998); see also *United States v. Rice*, 52 F.3d 843, 851 (10th Cir. 1995) (noting that both enhancements may be applied because "each of these enhancements serves a distinct purpose").

The commentary provides some guidance as to what qualifies as a special skill:

> "Special skill" refers to a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts.

U.S.S.G. § 3B1.3, cmt. n.4. As courts have noted, however, "[a] defendant does not need to have formal education or professional stature to have a special skill within the meaning of § 3B1.3[;] a special skill can be derived from experience or from self-tutelage." *United States v. Nelson-Rodriguez*, 319 F.3d 12, 58 (1st Cir. 2003) (quoting *United States v. Noah*, 130 F.3d 490, 500 (1st Cir. 1997); *see also United States v. Urban*, 140 F.3d 229, 236 (1st Cir. 1998) ("[A] § 3B1.3 sentence enhancement is not limited to persons who have received substantial

formal education, training from experts, or who have been licensed to perform a special skill.").

The inquiry regarding whether a particular skill constitutes a "special skill" for the purposes of § 3B1.3 is intensely fact specific. The metric of comparison by which it is determined whether a skill is "special," i.e., the skill possessed by the general public, may also evolve over time and vary from one community to another. As a result, courts have not spoken with a clear voice regarding what qualifies as a special skill. Courts have upheld imposition of the enhancement upon a mechanical drafter whose knowledge of "complex" drafting software facilitated his theft of trade secrets (see *United States v. Lange*, 312 F.3d 263, 270 (7th Cir. 2002)) and upon an intruder who demonstrated an ability to "bypass security protocols to gain access to computer systems" (*see United States v. Petersen*, 98 F.3d 502, 508 n.5 (9th Cir. 1996) (noting that imposition of the enhancement is appropriate "[o]nly where a defendant's computer skills are particularly sophisticated")). On the other hand, courts have overturned application of the special skill enhancement to a defendant who copied and modified webpage source code to facilitate a fraud scheme (*see United States v. Lee*, 296 F.3d 792, 799 (9th Cir. 2002)) and a defendant who used off-the-shelf software to produce counterfeit currency (see *United States v. Godman*, 223 F.3d 320, 323 (6th Cir. 2000)). If there is coherent precedent to be gleaned from this case law, it is that the government must present to the sentencing court considerable evidence that the defendant's uncommon ability facilitated the commission or concealment of the crime.

F. Conditions of Supervised Release

Increasingly, prosecutors, parole officers, and courts struggle to impose appropriate conditions on the Internet use of defendants whose sentences include terms of supervised release. Courts have circumscribed discretion in imposing such conditions—they may fashion any remedy that takes into consideration certain enumerated criteria. *See United States v. Holm*, 326 F.3d 872, 876 (7th Cir. 2003); *United States v. White*, 244 F.3d 1199, 1204 (10th Cir. 2001); *see also* 18 U.S.C. §§ 3583(c), 3553 (enumerating the criteria). Of particular relevance to computer crimes, courts must consider the need for the sentence imposed "to afford adequate deterrence to criminal conduct" and "to protect the public from further crimes of the defendant." 18 U.S.C. § 3553(a)(2)(B), (a)(2)(C). Where a networked computer has been used to perpetrate online fraud, to receive contraband such as child pornography or

stolen credit card numbers, or as the instrument of intrusions into or attacks on other computers, these considerations may militate in favor of imposing a restriction on computer use as a condition of supervised release.

Section 3553(a) requires all conditions of supervised release to impose upon a defendant "no greater deprivation of liberty than is reasonably necessary to achieve" a valid penological purpose. *Holm*, 326 F.3d at 876; *White*, 244 F.3d at 1204-05. When such conditions affect a defendant's use of the Internet, a recognized forum for First Amendment activity, this statutory requirement takes on constitutional implications. *See United States v. Scott*, 316 F.3d 733, 736 (7th Cir. 2003); *see generally ACLU v. Reno*, 521 U.S. 844 (1997). On a more pragmatic level, courts have noted that in an era when the Internet is a prevalent means of communication, source of information, and medium for commercial transactions and the provision of public services, "a strict ban on all Internet use ... renders modern life ... exceptionally difficult." *Holm*, 326 F.3d at 878.

As a result, appellate courts have routinely struck down conditions of supervised release that infringe upon a defendant's Internet use more than necessary, and admonished sentencing courts and parole officers to tailor the conditions more narrowly to the end to be served. *See, e.g., United States v. Freeman*, 316 F.3d 386, 392 (3d Cir. 2003); *Scott*, 316 F.3d at 737 (suggesting as an alternative to a total ban on Internet use unannounced inspections of a defendant's computer); *Holm*, 326 F.3d at 879 (suggesting random searches of a defendant's computer and use of filtering software as an appropriate condition for a defendant convicted of possessing child pornography); *White*, 244 F.3d at 1204-07. At least one court has suggested, however, that a total ban may be appropriate where a defendant's crime involves using a computer to attack or intrude upon others' networks. *See Scott*, 316 F.3d at 736 (dicta) (Inveterate intruders who have used access to injure others may be ordered to give up the digital world."). Similarly, courts have not hesitated to uphold limitations on computer use that are appropriately circumscribed. *See United States v. Ristine*, 335 F.3d 692 (8th Cir. 2003); *United States v. Crandon*, 173 F.3d 122 (3d Cir. 1999).

These cases suggest that prosecutors and parole officers should work together to propose to sentencing courts conditions of supervised release that achieve their objectives while infringing upon defendants' legitimate Internet use with care. They also suggest, however, that if such conditions are reasonably

crafted to be respectful of defendants' liberties, they are appropriate and will be upheld.

Appendix A
Unlawful Online Conduct and Applicable Federal Laws

The chart below details the type of unlawful online conduct, potentially applicable federal laws, and the section of the Department of Justice with subject-matter expertise. If the subject matter expert is not a section of the Department, but rather another agency, the entry will have an asterisk following its initials.

In many cases, prosecutors may also consider whether the conduct at issue is a violation of 18 U.S.C. § 2 (aiding and abetting) or 18 U.S.C. § 371 (conspiracy).

Unlawful Conduct	Applicable Federal Law	DOJ Section
Denial of Service Attacks	18 U.S.C. § 1030(a)(5)(A) (transmission of program, information, code, or command, resulting in damage)	CCIPS
	18 U.S.C. § 1362 (interfering with government communication systems)	CCIPS
Substitution or Redirection of a website	18 U.S.C. § 1030(a)(5)(A)(i) (transmission of program, information, code, or command, resulting in damage)	CCIPS
	18 U.S.C. § 1030(a)(5)(A)(ii)-(iii) (accessing a computer without authorization, resulting in damage)	CCIPS
Use of Misleading Domain Name	18 U.S.C. § 2252B (using misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material)	CEOS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Extortion	18 U.S.C. § 1030(a)(7) (transmitting, with intent to extort, communication containing threat to cause damage)	CCIPS
	18 U.S.C. § 875(b), (d) (transmitting, with intent to extort, threat to kidnap or harm a person, or threat to injure a person's property or harm a reputation) (Hobbs Act)	CTS
	18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence)	DSS
Internet Fraud (e.g., auction fraud or "phishing")	18 U.S.C. § 1030(a)(4) (accessing a computer to defraud and obtain something of value)	CCIPS
	18 U.S.C. § 1028 (fraud in connection with identification documents and authentication features)	Fraud
	18 U.S.C. § 1028A (aggravated identity theft)	Fraud
	18 U.S.C. § 1343 (wire fraud)	Fraud
	18 U.S.C. §§ 1956, 1957 (money laundering)	AFMLS
	18 U.S.C. § 1001 (making false statements in any matter within the jurisdiction of the government)	Fraud
	15 U.S.C. § 45 (unfair or deceptive trade practices)	*FTC
	15 U.S.C. § 52 (false advertising)	*FTC
	15 U.S.C. § 6821 (fraudulent access to financial information)	*FTC/Fraud

Unlawful Conduct	Applicable Federal Law	DOJ Section
Credit Card Fraud	18 U.S.C. § 1030(a)(2)(A) (accessing a computer and obtaining information from a financial institution, card issuer or consumer reporting agency)	CCIPS
	18 U.S.C. § 1029 (access device fraud)	Fraud/CCIPS
	15 U.S.C. § 1644 (credit card fraud aggregating at least $1,000)	Fraud
	18 U.S.C. § 1343 (wire fraud)	Fraud
Password Fraud	18 U.S.C. § 1030(a)(6) (trafficking in computer passwords)	CCIPS
	18 U.S.C. § 1029 (access device fraud)	Fraud/CCIPS
	18 U.S.C. § 1343 (wire fraud)	Fraud
Child Pornography, Child Luring, and Related Activities	18 U.S.C. §§ 2251, 2252, 2252A (sexual exploitation of children)	CEOS
	18 U.S.C. § 2423 (transportation of minors or travel with intent to engage in illicit sexual conduct)	CEOS
	18 U.S.C. § 1466A (obscene visual representations of the sexual abuse of children)	CEOS
Obscenity	47 U.S.C. § 223(a)(1)(A) (using telecommunications device to make, create, or solicit, and transmit any obscene comment, request, suggestion, proposal, image, or other communication)	CEOS
	18 U.S.C. § 1465 (using interactive computer service for purpose of sale or distribution of obscene material)	CEOS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Sale of Prescription Drugs and Controlled Substances	15 U.S.C. § 45 (unfair or deceptive trade practices)	*FTC
	15 U.S.C. § 52 (false advertising)	*FTC
	18 U.S.C. § 545 (smuggling goods into the United States)	Fraud/AFMLS
	18 U.S.C. § 1343 (wire fraud)	Fraud
	21 U.S.C. §§ 301 et seq. (Federal Food, Drug, and Cosmetic Act)	*FDA
	21 U.S.C. §§ 822, 829, 841, 863, 951-71 (Drug Abuse Prevention and Control)	Fraud/NDDS
	18 U.S.C. § 2320 (trafficking in counterfeit goods or services)	CCIPS
Sale of Firearms	18 U.S.C. § 922 (unlawful sale of firearms)	DSS
Gambling	15 U.S.C. §§ 3001 et seq. (Interstate Horseracing Act)	OCRS
	18 U.S.C. § 1084 (use of wire communication facility to transmit bets or wagering information)	OCRS
	18 U.S.C. § 1301 (importing or transporting lottery tickets)	OCRS/AFMLS
	18 U.S.C. § 1952 (use of facilities in interstate or foreign commerce to aid in racketeering enterprises)	OCRS
	18 U.S.C. § 1953 (interstate transportation of wagering paraphernalia)	OCRS
	18 U.S.C. § 1955 (conducting, financing, managing, supervising, directing, or owning an illegal gambling business)	OCRS/AFMLS
	28 U.S.C. § 3701 et seq. (Professional and Amateur Sports Protection Act)	OCRS/AFMLS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Sale of Alcohol	18 U.S.C. §§ 1261 et seq. (transportation of liquor into state prohibiting sale; shipping liquor without required marks and labels on package)	OCRS/Treasury
	27 U.S.C. §§ 122, 204 (interstate shipping of alcohol)	OCRS/Treasury
Securities Fraud	15 U.S.C. §§ 77e, 77j, 77q, 77x, 78i, 78j, 78l, 78o, 78ff (securities fraud)	Fraud/SEC
	18 U.S.C. § 1343 (wire fraud)	Fraud/CCIPS
Piracy and Intellectual Property Theft	17 U.S.C. §§ 1201-1205 (Digital Millennium Copyright Act)	CCIPS
	18 U.S.C. § 545 (smuggling goods into the United States)	AFMLS
	18 U.S.C. §§ 1831, 1832 (theft of trade secrets)	CES/CCIPS
	18 U.S.C. § 2318 (trafficking in counterfeit labels)	CCIPS
	17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal copyright infringement)	CCIPS
	18 U.S.C. § 2319A (trafficking in recordings of live musical performances)	CCIPS
	18 U.S.C. § 2320 (trafficking in counterfeit goods or services)	CCIPS
	47 U.S.C. § 553 (unauthorized reception of cable service)	Fraud
	18 U.S.C. § 1343 (wire fraud)	Fraud

Unlawful Conduct	Applicable Federal Law	DOJ Section
Trade Secrets/ Economic Espionage	18 U.S.C. § 1831 (theft of trade secrets for benefit of foreign government)	CES/CCIPS
	18 U.S.C. § 1832 (theft of trade secrets)	CCIPS
	18 U.S.C. § 1905 (disclosure of confidential information)	Public Integrity
	18 U.S.C. §§ 2314, 2315 (interstate transportation or receipt of stolen property)	OEO
Electronic Threats	18 U.S.C. § 875 (transmitting communications containing threats of kidnap or bodily injury) (Hobbs Act)	CTS
	18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence) (Hobbs Act)	DSS
	47 U.S.C. § 223 (a)(1)(C) (anonymously using telecommunications device to threaten person who receives communication)	CCIPS
Electronic Harassment	47 U.S.C. § 223 (a)(1)(C) (anonymously using telecommunications device to harass person who receives communication)	CCIPS
	47 U.S.C. § 223(a)(1)(E) (repeatedly initiates communication with a telecommunication device solely to harass person who receives communication)	CCIPS
Interception of Electronic Communications	18 U.S.C. § 2511 (intercepting electronic communications)	CCIPS
	18 U.S.C. § 2701 (accessing stored communications)	CCIPS
	18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information)	CCIPS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Cyberstalking	18 U.S.C. § 2261A (using any facility of interstate or foreign commerce to engage in a course of conduct that places person in reasonable fear of death or serious bodily injury to person, person's spouse or immediate family) See also *Electronic Harassment*	DSS
Espionage	18 U.S.C. § 1030(a)(1) (accessing a computer and obtaining national security information)	CES
	18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information from any department or agency of the United States)	CCIPS
	18 U.S.C. § 1030(a)(3) (accessing a nonpublic United States government computer)	CCIPS
	18 U.S.C. § 793 (gathering, transmitting or losing defense information)	CES
	18 U.S.C. § 798 (disclosing classified information)	CES
Hate Crimes	Look to civil rights laws and penalty enhancements	Civil Rights
Libel/Slander	Look to civil laws	
Posting Personal Information on a Website (e.g., phone numbers, addresses)	This is not a violation of law. May also be protected speech under First Amendment.	
Invasion of Privacy	See *Interception of Electronic Communications*	
Disclosure of Private Information	18 U.S.C. § 2511(1)(c) (disclosing intercepted communications)	CCIPS
Spam	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS
Spoofing Email Address	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS

Appendix B
Best Practices for Working with Companies

Intrusion crimes can damage or impair the functioning of computers and networks. Victims may be the intended targets of the intrusion or third parties whose systems are used to carry out unlawful activity, such as universities and Internet service providers. After a company reports an intrusion, there are a number of "best practices" for law enforcement that can make the relationship between law enforcement and companies more productive in the aftermath of a computer incident. The practices discussed here are designed to be implemented in addition to, not in lieu of, the Attorney General Guidelines for Victim and Witness Assistance.[1] Also, please note that the Secret Service publishes a guide on the mechanics of seizing computer evidence, *Best Practices for Seizing Electronic Evidence, available at* http://www.forwardedge2.com/pdf/bestPractices.pdf.

Because computer information systems are essential to the everyday operation of most businesses, the disruption of those services can cripple a company. Law enforcement should remain aware of the tension between their need to collect evidence for prosecution and the company's need to resume operations as quickly as possible. Also, companies usually wish to avoid the negative publicity frequently associated with a breach of network security.

Because victims play an important role in providing computer logs and factual testimony regarding the intrusion, we also suggest some "best practices" for companies to consider when responding to a network crime. These suggested practices are in Appendix C.

In general, law enforcement should seek to build a trusted relationship with companies. Keeping these goals in mind will help to obtain timely assistance from companies and increase the likelihood of successful prosecutions.

[1] The current copy of the Attorney General Guidelines for Victim and Witness Assistance can found at: http://www.ojp.usdoj.gov/ovc/publications/welcome.html.

1. Protect the Rights of the Victim

Law enforcement should ensure that the victim's rights under 18 U.S.C. § 3771(a) are honored, including the rights to

- reasonable protection from the accused
- accurate and timely notice of court proceedings involving the crime or of any release or escape of the accused
- not be excluded from any such public court proceeding, unless the court determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding
- be heard at any public proceeding in the district court involving release, plea, sentencing, or probation
- confer with the government attorney on the case
- full and timely restitution as provided in law
- proceedings free from unreasonable delay
- be treated with fairness and with respect for the victim's dignity and privacy

2. Consult with Senior Management

Consulting with the company's senior management before undertaking investigative measures on the company's network will often pay dividends. Some decisions require the authorization of a company's senior management. For example, system administrators may lack authority to consent to law enforcement activities that will affect business operations. In addition, be aware that if the company or its employees are represented by legal counsel in the matter, direct contact with those persons may be restricted absent the attorney's consent. This ethical constraint binds Department of Justice attorneys as well as the agents operating on their behalf.

3. Consult with Information Technology Staff

Whenever possible, we suggest consulting with the company's information technology staff about network architecture before implementing investigative measures on the network. Working closely with the information technology staff will help to obtain important information, including information regarding network topology. Helpful information will include the type and version of software being run on the network and any peculiarities in the architecture of the network, such as proprietary hardware or software. Obtaining this information will help to ensure that law enforcement can obtain all information relevant

to an investigation and minimize disruption of the company's network from investigative measures.

Specific things to identify in a network include the locations of intrusion detection systems, network switches, and firewalls. Also, identify all data logs, including the type data being logged, the size of the log files (to check for losing data due to rolling retention), and location of the logs (sent to a log server or maintained on the hacked system and subject to compromise themselves).

4. Minimize Disruption to the Company

Law enforcement should make every effort to use investigative measures that minimize computer downtime and displacement of a company's employees. Some investigative measures are indispensable despite the inconvenience to a company. Other investigative steps may be altered or avoided if they needlessly aggravate employees or prolong the damage already suffered by a company. For example, rather than seizing compromised computers and depriving the company of their use, consider creating a "mirror image" of the system and leaving computers in place. Also, consider practical issues such as whether raid jackets or other insignia are appropriate to display.

Similarly, although consulting with company system administrators and computer experts is essential, avoiding excessive burdens on these personnel can help promote the trust and goodwill of company.

5. Coordinate Media Releases

Investigations and prosecutions of cybercrime cases may entail the release of information by law enforcement in press releases or press conferences. All press releases and press conferences should be coordinated with the Office of Public Affairs at (202) 514-2007.

Additionally, public statements to the news media should also be coordinated with the company to ensure that these statements do not needlessly reveal information harmful to a company. Informing companies of this coordination at an early stage in the investigation is an important step. Fear of damage to carefully built reputations is a major reason why companies refrain from reporting crime to law enforcement. Law enforcement should take all possible

measures to prevent unauthorized releases of information about pending investigations and to punish unauthorized disclosures when they occur.

In return, consider asking the company to allow the investigating agents to review any press releases regarding the investigation before issuing them. This will prevent the company from releasing information that could damage the investigation.

6. Keep the Company Informed About the Investigation

After conducting the initial on-site investigation, law enforcement may have little direct contact with a company. To the extent possible—recognizing the need to guard against disclosure of grand jury information or information that could otherwise jeopardize the investigation—keep the company informed of the progress of the investigation. In addition, where an arrest is made that results in court proceedings, notify the company of all significant court dates so company personnel have the opportunity to attend.

7. Build Relationships Before an Intrusion

Many companies, universities, and other victims are reluctant to report cybercrime incidents to law enforcement because they are fearful that law enforcement will conduct an investigation in a manner harmful to their operational interests or because they have misconceptions about how law enforcement will conduct an investigation. Such fears and misconceptions can more easily be dispelled if law enforcement has a pre-existing relationship with a company, rather than having the company's first contact with law enforcement come in the midst of a crisis. For example, forming liaison groups comprised of law enforcement and private industry representatives can help bridge gaps of mistrust or unfamiliarity and increase future cybercrime reporting by private industry.

Appendix C
Best Practices for Victim Response and Reporting

A quick and effective response by a company is critical for stopping an ongoing attack and preventing future attacks. Moreover, the use of established procedures—including preservation of evidence—and notification to incident-reporting organizations and/or to law enforcement will help to secure systems of other victims or potential victims. Use of the practices discussed below by companies may help to minimize damage to computer networks from attacks and maximize opportunities to find the attacker.

Because victims play an important role in providing computer logs and factual testimony regarding the intrusion, we also suggest some "best practices" for companies to consider when responding to a network crime, including reporting incidents to law enforcement and to data subjects. Companies, universities, and other organizations should consider these practices as part of their contingency planning before they are attacked, so they are prepared to respond appropriately when attacked.

While these practices are designed to assist network operators and system administrators, it is important for investigators and prosecutors to be familiar with these practices as well. For first-time victims, law enforcement can offer advice on prudent steps the victim should take. Law enforcement also may have opportunities for outreach to organizations that are considering contingency planning for future network attacks or to organizations that are considering remedial steps (e.g., changes to company procedures) after they have responded to a network crime.

A. Steps Before Confronting an Intrusion

1. Be Familiar with Procedures, Practices, and Contacts

Organizations should have procedures in place to handle computer incidents. These procedures should be reviewed periodically and made available to all personnel who have system security responsibilities. The procedures should

provide specific guidance to follow in the event of a computer incident. Ideally, those procedures should specify: who in the organization has lead responsibility for internal incident response; who are the points-of-contact inside and outside the organization; what criteria will be used to ascertain whether data owners or subjects of any data taken by the attackers must be notified; and at what point law enforcement and a computer incident-reporting organization should be notified.

2. Consider Using Banners

Real-time monitoring of attacks is usually lawful, if prior notice of this monitoring is given to all users. For this reason, organizations should consider deploying written warnings, or "banners," on the ports through which an intruder is likely to access the organization's system and on which the organization may attempt to monitor an intruder's communications and traffic. If a banner is already in place, it should be reviewed periodically to ensure that it is appropriate for the type of potential monitoring that could be used in response to a cyberattack. More information on this topic can be found on CCIPS' website at http://www.cybercrime.gov.

B. Responding to a Computer Incident

1. Make an Initial Identification and Assessment

A first step for an organizations is to make an initial identification of the type of incident that has occurred or is occurring, and to confirm that it is, in fact, an incident. The network administrator should determine the nature and scope of the problem—i.e., which specific systems were affected and in what ways they were affected. Indicators that an intrusion or other incident has occurred will typically include evidence that files or logs were accessed, created, modified, deleted or copied, or that user accounts or permissions have been added or altered. In the case of a root-level intrusion, attention should be paid to any signs that the intruder has gained access to multiple areas of the system—some of which may remain undetected. Using network log information, the system administrator should determine (a) the immediate

origin of the attack; (b) the identity of servers to which the data were sent (if information was transferred); and (c) the identity of any other victims. Care should be taken to ensure that such initial actions do not unintentionally modify system operations or stored data in a way that could compromise the incident response—including a subsequent investigation.

2. Take Steps to Minimize Continuing Damage

After the scope of the incident has been determined, an organizations may need to take certain steps to stop continuing damage from an ongoing assault on its network. Such steps may include installing filters to block a denial of service attack or isolating all or parts of the system. In the case of unauthorized access or access that exceeds user authorization, a system administrator may decide either to block further illegal access or to watch the illegal activity in order to identify the source of the attack and/or learn the scope of the compromise.

Initial response should include at a minimum documenting: users currently logged on, current connections, processes running, all listening sockets and their associated applications.

Image the RAM of the attacked systems.

As described below, detailed records should be kept of whatever steps are taken to mitigate the damage flowing from an attack and any associated costs incurred as a result. Such information may be important for recovery of damages from responsible parties and for any subsequent criminal investigation.

3. Notify Law Enforcement

If at any point during the organization's response or investigation it suspects that the incident constitutes criminal activity, law enforcement should be contacted immediately. To the extent permitted by law, information already gathered should be shared with law enforcement. As noted above, certain state laws may allow a company that reports an intrusion to law enforcement to delay providing notice to data-subjects if such notice would impede a law enforcement investigation.

Companies should note that law enforcement has legal tools that are typically unavailable to victims of attack; these tools can greatly increase the chances of identifying and apprehending the attacker. When law enforcement arrests and successfully prosecutes an intruder, that intruder is deterred from

future assaults on the victim. This is a result that technical fixes to the network cannot duplicate with the same effectiveness.

Intrusion victims may believe that they can block out an intruder by fixing the exploited vulnerability. However, it is not uncommon for an intruder to install a "back door" through which he can continue to access the system after the initial point of compromise is repaired. Catching and prosecuting the intruder may be the only method to truly secure the organization's system from future attacks by the culprit.

In addition, by using the criminal justice system to punish the intruder, other would-be intruders may be deterred from attacking the organization's networks. Criminal law enforcement can thus play a significant and long-term role in network security.

4. Do Not Hack into or Damage the Source Computer

Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as "hacking back" into the attacker's computer—even if such measures could in theory be characterized as "defensive." Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, "hacking back" can damage the system of another innocent party. If appropriate, however, the company's system administrator can contact the system administrator from the attacking computer to request assistance in stopping the attack or in determining its true point of origin.

5. Record and Collect Information

Mirror Image

A system administrator for the company should consider making an immediate identical copy of the affected system, which will preserve a record of the system at the time of the incident for later analysis. This copy should be a "system level" or "zero level" copy and not just a copy of user files. In addition, any previously-generated backup files should be located. New or sanitized media should be used to store copies of any data which is retrieved and stored. Once such copies are made, the media should be write-protected to guard it from alteration. In addition, access to this media should be controlled to maintain the integrity of the copy's authenticity, to keep undetected insiders away from it, and to establish a simple chain of custody. These steps will enhance the value

of any backups as evidence in any later internal investigations, civil suits, or criminal prosecutions.

Notes, Records, and Data

As the investigation progresses, information that was collected by the company contemporaneous to the events may take on great significance. Immediate steps should be taken to preserve relevant logs that already exist. In addition, those persons participating in the incident response should be directed to keep an ongoing, written record of all steps undertaken. If this is done at or near the time of the events, the participants can minimize the need to rely on their memories or the memories of others to reconstruct the order of events.

The types of information that should be recorded by the company include:

- description of all incident-related events, including dates and times
- information about incident-related phone calls, emails and other contacts
- the identity of persons working on tasks related to the intrusion, including a description, the amount of time spent, and the approximate hourly rate for those persons' work
- identity of the systems, accounts, services, data, and networks affected by the incident, and a description of how these network components were affected
- information relating to the amount and type of damage inflicted by the incident, which can be important in civil actions by the company and in criminal cases.

Ideally, a single person should be provided copies of all such records. This will help to ensure that the records are properly preserved and capable of being produced later on. It is often crucial to the success of a legal proceeding to defeat any claim that records or other evidence may have been altered subsequent to their creation. This is best accomplished by establishing a continuous "chain of custody" from the time that records were made until the time they were brought into the court.

6. Record and Log Continuing Attacks

When an attack is ongoing or when a system has been infected by a virus or worm, this continuing activity should be recorded or logged by the victim. *If logging is not underway, it should begin immediately.* Increase default log file size to prevent losing data. A system administrator may be able to use a "sniffer" or other monitoring device to record communications between the intruder and any server that is under attack. Such monitoring is usually permissible, provided that it is done to protect the rights and property of the system under attack, the user specifically consented to such monitoring, or implied consent was obtained from the intruder—e.g., by means of notice or a "banner." More guidance on banners can be found in our manual *Searching and Seizing computers and Obtaining Electronic Evidence in Criminal Investigations* (2d ed. 2002).

A banner should notify users or intruders as they access or log into a system that their continued use of the system constitutes their consent to being monitored and that the results of such monitoring may be disclosed to law enforcement and others. Legal counsel at the company should be consulted to make sure such monitoring is consistent with employment agreements, privacy policies, and legal authorities and obligations.

7. Do Not Use the Compromised System to Communicate

The company should avoid, to the extent reasonably possible, using a system suspected of being compromised to communicate about an incident or to discuss incident response. If the compromised system must be used to communicate, all relevant communications should be encrypted. To avoid being the victim of social engineering and risking further damage to the organization's network, employees of the company should not disclose incident-specific information to callers who are not known points-of-contact, unless the employee can verify the identity and authority of those persons. Suspicious calls, emails, or other requests for information should be treated as part of the incident investigation.

8. Notify

People Within the Organization

Appropriate people in the organization should be notified immediately about the incident and provided with the results of any preliminary investigation.

This may include security coordinators, managers, and legal counsel. (A written policy for incident response should set out points-of-contact within the organization and the circumstances for contacting them.) When making these contacts, only protected or reliable channels of communication should be used. If the company suspects that the perpetrator of an attack is an insider, or may have insider information, the company may wish to strictly limit incident information to a need-to-know basis.

Computer Incident-reporting Organization

Whenever possible, the company should notify an incident-reporting organization, such as a Computer Emergency Response Team (CERT). Reporting the incident and the means of attack may help to hamper the attacker's ability to replicate the intrusion against other target systems.

The United States Computer Emergency Response Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT is charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States government about cyber security. Reporting intrusions may not only help protect the company's system from further damage, it could also help to alert other actual or potential victims who otherwise might not be aware of the suspicious activity. They can be contacted on the Internet at http://www.us-cert.gov.

Other Potential Victims

If there is another organization, or a vulnerability in a vendor's product that is being exploited, it may be prudent for the company to notify the victim or vendor—or request that an incident-reporting organization or CERT alert the victim or vendor. The third-party victim or vendor may be able to provide new and previously unknown information about the incident (e.g., hidden code, ongoing investigations in other areas, or network configuration techniques). Such notification may prevent further damage to other systems.

Note also that state laws may require companies to notify people whose data is compromised during an intrusion. For example, California law requires that:

> [a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Cal. Civil Code § 1798.82(a). As of July 2006, thirty-four states have passed database breach notification laws.[1] Some of the state laws allow for notice to be delayed if it would impede a criminal investigation.[2]

At least one state law allows the database owner to elect against providing notice to data subjects if the database owner consults with law enforcement and thereafter determines that the breach "will not likely result in harm to the individuals whose personal information has been acquired and accessed."[3] A number of federal bills are currently pending, many of which would preempt existing state laws.

C. After a Computer Incident

A critical action after an intrusion and its associated investigation are complete is to take steps to prevent similar attacks from happening again. In order to keep similar incidents from occurring, victims should do conduct a post-incident review of the organization's response to the attack and assessment of the strengths and weaknesses of this response. Part of the assessment should include ascertaining whether each of the steps outlined above occurred.

---

[1] State PIRG Summary of State Security Freeze and Security Breach Notification Laws, *available at*: http://www.pirg.org/consumer/credit/statelaws.htm (visited October 12, 2006).

[2] Fla. Stat. § 817.5681(3) (2005); Conn. S.B. 650 § 3(d).

[3] Conn. S.B. 650 § 3(b).

Appendix D
Network Crime Resources

A. Federal Law Enforcement Contacts

Computer Crime and Intellectual Property Section (CCIPS)
Criminal Division, U.S. Department of Justice
1301 New York Avenue, N.W., Suite 600
Washington, DC 20530
Tel: 202-514-1026
Fax: 202-514-6113
http://www.cybercrime.gov
http://www.usdoj.gov

Prosecution of, and guidance, support, resources, and materials for prosecuting domestic and international network crime offenses; development of network crime policy; and support and coordination of the federal prosecution of network crimes.

Federal Bureau of Investigation
Cyber Intrusion Division
J. Edgar Hoover FBI Building
935 Pennsylvania Avenue, N.W.
Washington, DC 20535
http://www.fbi.gov
Tel: 202-324-5613
Fax: 202-324-9197

Responsible for all network crime investigations. For a list of field offices, see http://www.fbi.gov/contact/fo/fo.htm.

United States Secret Service
Criminal Investigation Division
Department of Homeland Security
950 H St., N.W.
Washington, DC 20223
202-406-9330
http://www.secretservice.gov

Investigative responsibilities include computer and telecommunications fraud, financial institution fraud, false identification documents, access device fraud, electronic funds transfers, and money laundering as it relates to these violations. For a list of field offices, see http://www.secretservice.gov/field _offices.shtml.

B. On the Web

Internet Crime Complaint Center (IC3)
1 Huntington Way
Fairmont, WV 26554
Tel: 800-251-3221; 304-363-4312; complaint center: 800-251-7581
Fax: 304-363-9065
http://www.ic3.gov

Partnership between NW3C and FBI. Allows victims to report fraud over the Internet; alerts authorities of suspected criminal or civil violations; offers law enforcement and regulatory agencies a central repository for complaints related to Internet fraud.

Cybercrime.gov

The CCIPS website, http://www.cybercrime.gov, provides information about the topics on which the Section focuses, including computer crime, intellectual property, electronic evidence, and other high-tech legal issues. The website includes news on recent criminal investigations and prosecutions in these areas, background information on cases, and speeches and testimony by Department of Justice officials. Also available on cybercrime.gov are legal research and reference materials on computer crime and intellectual property, including three manuals for prosecutors and law enforcement published by CCIPS on intellectual property, electronic evidence, and this manual.

C. Publications

U.S. Department of Justice, *Searching and Seizing Computers and Electronic Evidence in Criminal Investigations* (Office of Legal Education 2002). Provides comprehensive guidance on compute-related search issues in criminal investigations. The topics covered include the application of the Fourth Amendment to computers and the Internet, the Electronic Communications Privacy Act, workplace privacy, the law of electronic surveillance, and evidentiary issues.

U.S. Department of Justice, *Prosecuting Intellectual Property Crimes* (Office of Legal Education 2006). Presents comprehensive descriptions and analysis of all federal criminal intellectual property laws, including copyright, trademark, theft of trade secrets, counterfeit labeling, the Digital Millennium Copyright Act, and alternative mainstream criminal statutes that can be applied to intellectual property theft, including mail and wire fraud, the Computer Fraud and Abuse Act, and the interstate transportation of stolen property statutes. This manual emphasizes practical suggestions for investigating such cases, anticipating defenses, dealing with victims and witnesses, and obtaining effective sentences.

U.S. Department of Justice, *Identity Theft and Social Security Fraud* (Office of Legal Education 2004). Authored by the Fraud Section of the Criminal Division, this manual includes detailed sections on prosecutions under 18 U.S.C. §§ 1028 (identity theft), 1029 (aggravated identity theft), and 1343 (mail fraud and wire fraud).

Best Practices for Seizing Electronic Evidence (3d ed.). A pocket guide published by the U.S. Secret Service for first responders to an electronic crime scene. This document is available at http://www.forwardedge2.com/pdf/bestPractices.pdf.

Index

A

Acquire/Acquisition 57, 58, 59, 60, 73, 79
Administration of justice 31, 37, 42, 43, 95, 120
Advertising 38, 40, 128, 130
Agency law 8
Agent 8, 10, 62, 63, 67, 68, 69, 96, 136, 138
Aggregate 39, 89
Anything of value 22, 23, 27, 28, 89
Attempt 2, 10, 11, 14, 43, 44, 59, 68, 91, 114, 121, 140

B

Back-door 36
Backup 38, 80, 81, 142
Bandwidth 29
Banner 6, 10, 72, 140, 144
Burglary 24

C

Civil action 3, 99, 143
Classified information 1, 11, 12, 13, 133
Code 2, 30, 31, 32, 33, 35, 36, 41, 52, 85, 114, 120, 124, 127, 145
Color of law 70, 72, 73, 74
Computer security. *See* Security
Confession 107
Confidentiality 6, 9, 21, 77
Consent 49, 62, 63, 70, 71, 72, 82, 96, 107, 136, 144
Conspiracy 16, 57, 127
Contractor 17, 43, 118
Copy [of email] 57, 60, 80, 81
Copy [files] 16, 28, 36, 37
Counterfeit 86, 113, 114, 117, 124, 130, 131, 149
Course of conduct 30, 39, 133
Credit card 24, 25, 47, 86, 94, 114, 118, 125, 129
Credit reporting 25

D

Database 20, 30, 35, 36, 37, 38, 49, 146
Death 14, 31, 43, 44, 99, 118, 133
Defraud 2, 5, 22, 23, 24, 25, 46, 47, 90, 114, 128
Denial of service 2, 29, 32, 35, 49
Device 48, 56, 57, 59, 60, 61, 62, 79, 85, 93, 94, 101, 113, 114, 117, 129, 132, 144, 148

E

Economic loss 37, 38, 43
Electronic communication 55, 56, 57, 58, 59, 60, 61, 63, 64, 66, 67, 68, 70, 74, 77, 78, 79, 80, 81, 82, 93, 102, 132, 133, 149
Electronic storage 58, 77, 79, 80, 81, 84
Employer policies 10
Executive Order 11, 12
Extension telephone 61, 62
Extradition 107
Extraterritorial 93, 94, 95

F

Falsified documents 25
Federal interest computer 3, 7
Fifth Amendment 104
Financial institution 1, 3, 4, 15, 29, 90, 94, 129, 148
First Amendment 65, 66, 125, 133
Foreign communication *See* Interstate or foreign communication
Foreign governments 14

Foreign nation 12
Fraud 1, 7, 22, 23, 24, 25, 26, 27, 29, 44, 68, 90, 93, 98, 101, 109, 115, 117, 118, 124, 128, 129, 130, 131, 148, 149

G

Good faith 56, 57, 74
Goodwill 28, 38, 40, 41, 113, 137
Government computer 1, 44, 107, 133

H

Home computer 35, 79
Hourly rate 38, 45, 143. *See also* Salary

I

Immunity 65
Implied consent 72, 144
Incident to the rendition 68, 70
Injury of the United States 11, 12, 13
Intangible goods/information 16
Integrity 21, 30, 34, 35, 36, 37, 44, 51, 77, 132, 142
Intelligence agencies 2
Intended loss 110, 111, 114, 115, 116
Intent to defraud 22, 23, 24, 46, 114
Intent to extort 49, 50, 128
Internal Revenue Service 6, 27
Interstate commerce 3, 33, 47, 52, 60, 93
Interstate or foreign commerce 3, 4, 46, 47, 49, 50, 59, 87, 90, 93, 94, 103, 130, 133
Interstate or foreign communication 15, 16, 17, 18, 93, 96
IP address 26, 87
ISP 28, 45

J

Jurisdiction 1, 17, 93, 94, 95, 98, 101, 102, 103, 128

K

Keylogger 35

L

Laptop 33
Licensee 9
Log 6, 35, 44, 52, 79, 137, 140, 143, 144
Long-distance 25, 69, 116
Lost sales 40
Lottery 25, 130

M

Mail 1, 7, 23, 24, 29, 49, 50, 57, 78, 87, 88, 91, 97, 98, 113, 119, 121, 149
Mail fraud 1, 23, 24, 29, 98, 149
Malicious code 2, 33
Medical care 31, 37, 41, 52
Member agreement 9
Military 43, 45, 91, 95, 118
Mistake of law 56, 57, 64, 74

N

National defense 11, 12, 13, 31, 37, 42, 43, 44, 120
National security 10, 11, 12, 13, 14, 31, 37, 42, 43, 120, 121, 133
National security information 10, 11, 12, 13, 14, 133
Nonpublic 20

O

Obtain information 6, 10, 15, 16, 17, 18, 25, 58, 96, 97, 119, 129, 132, 133
Ordinary course 61, 62, 63, 69

P

Packets 32, 97
Party 65, 66, 70, 71, 72, 73, 82, 119, 142, 145
Password 2, 6, 8, 10, 27, 34, 41, 45, 46, 47, 48, 52, 53, 67, 79, 86, 114, 117, 118, 129
Physical injury 30, 31, 37, 42, 51, 53
Predicate offense 14, 85, 90
Profit 40, 46
Protected computer 3, 4, 5, 9, 15, 16, 17, 22, 23, 24, 25, 28, 30, 31, 32, 33, 34, 43, 44, 49, 50, 72, 73, 87, 93, 96, 113
Provider exception 68, 69
Public figure 65
Public health 31, 37, 38, 42, 51, 120, 121

R

Reputation 28, 38, 40, 41, 128
Resecure 38, 40, 45
Restoring 38, 40, 41, 45, 46, 111, 112
RICO 14, 90
Rights and property 68, 69, 144
Robbery 24, 128, 132

S

Salary 38, 40, 45. *See also* Hourly rate
Scheme to defraud 2, 23
Security [of computer] 3, 11, 29, 34, 35, 38, 40, 44, 51, 124
Serious bodily injury 14, 43, 99, 118, 133
Social security number 84, 90, 118
Software license 9, 10
Spyware 58
Substantial nexus 69
Supervised release 14, 75, 124, 125
Switchboard operator 69
System administrator 36, 38, 41, 53, 70, 140, 141, 142, 144

T

Telephone 17, 25, 42, 50, 61, 62, 63, 65, 66, 69, 91, 93, 100, 116
Telephone company 25, 69, 93
Terrorism 14, 85, 90, 122
Theft 2, 16, 17, 24, 28, 68, 84, 85, 109, 124, 128, 131, 132, 149
Threat 2, 5, 23, 31, 37, 38, 42, 49, 50, 51, 65, 69, 103, 128, 132
Trade secret 8, 37, 66, 124, 131, 132, 149
Traffic/Trafficking 2, 42, 46, 47, 86, 117, 129, 130, 131, 140
Transmission 10, 14, 30, 31, 32, 33, 49, 52, 55, 57, 58, 60, 68, 69, 80, 81, 87, 89, 90, 91, 93, 97, 98, 102, 103, 120, 121, 122, 127
Transmit 11, 12, 13, 14, 49, 60, 71, 78, 90, 129, 130
Trespass/Trespasser 1, 5, 10, 17, 19, 20, 21, 25, 26, 36, 72, 73, 74, 101

U

URL 36, 59
USA PATRIOT Act 2, 4, 14, 45, 51, 94
User agreement 6, 10

V

Venue 95, 96, 97, 98
Virus 29, 36, 39, 102, 115, 143
Voicemail 77, 78, 79, 80, 81

W

Waive/Waiver 95, 96, 105
Wire fraud 22, 23, 24, 27, 29, 90, 98, 128, 129, 130, 131, 149
Worm 7, 8, 29, 32, 34, 39, 143