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)

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.

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

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)

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.*

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

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)

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).

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

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–

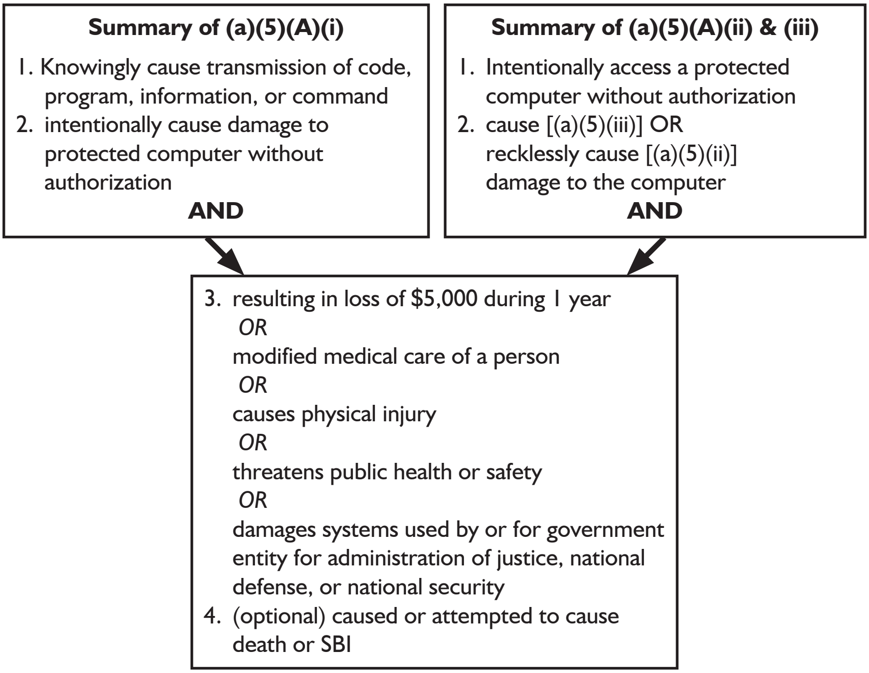
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(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;*



Summary of (a)(5)(A)(i)

1. Knowingly cause transmission of code, program, information, or command
2. intentionally cause damage to protected computer without authorization

AND

Summary of (a)(5)(A)(ii) & (iii)

1. Intentionally access a protected computer without authorization
2. cause [(a)(5)(iii)] OR recklessly cause [(a)(5)(ii)] damage to the computer

AND

3. resulting in loss of $5,000 during 1 year
   OR
   modified medical care of a person
   OR
   causes physical injury
   OR
   threatens public health or safety
   OR
   damages systems used by or for government entity for administration of justice, national defense, or national security
4. (optional) caused or attempted to cause death or SBI

> *(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.