THE NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1996

LEGISLATIVE ANALYSIS

By

The Computer Crime and Intellectual Property Section
United States Department of Justice

Also see Computer Crime and Intellectual Property Section, U.S. Department of Justice, Legislative Analysis of the 1996 National Information Infrastructure Protection Act, 2 Electronic Info. Pol'y & L. Rep. 240, 240 (1997).

I. INTRODUCTION: The Need for Legislative Reform

Although there has never been accurate nationwide reporting of computer crime, it is clear from the reports which do exist and from anecdotal information that computer crime is on the rise. For example, the Computer Emergency and Response Team at Carnegie-Mellon University reports that from 1991 through 1994, there was a 498% increase in the number of computer intrusions, and a 702% rise in the number of sites affected. See CERT Annual Report to ARPA. During 1994, for example, approximately 40,000 Internet computers were attacked in 2,460 incidents. Id. Similarly, the FBI's National Computer Crime Squad has opened over 200 hacker cases since the Squad was created in 1991.

That computer crime is on the rise is perhaps a natural result of introducing computers into American society. In an earlier era, the advent of the automobile opened the way for criminals to target the automobile itself (e.g., auto theft) or use it to facilitate traditional crimes (e.g., the bank robbery getaway vehicle). In addition, law enforcement had to learn to seize vehicles to search them for evidence of some offense unrelated to the vehicle itself (e.g., the box of documents in the trunk). In many of the same ways, computers, too, have proven important to criminal investigations. First, a computer may be the target of the offense. In these cases, the criminal's goal is to steal information from, or cause damage to, a computer, computer system, or computer network. Second, the computer may be a tool of the offense. This occurs when an individual uses a computer to facilitate some traditional offense such as fraud (e.g., a bank teller who once stole money from a cash drawer may now use a computer program to skim money directly from depositors' accounts). Last, computers are sometimes incidental to the offense, but significant to law enforcement because they contain evidence of a crime. Narcotics dealers, for example, may use a personal computer to store records pertaining to drug trafficking instead of relying on old-fashioned ledgers.

The different ways in which criminals can use computers have created a philosophical debate among law enforcement experts. Some argue that computer crime is nothing more than traditional crime committed with new, high-tech devices. Others contend that computer

crime cannot be analogized to traditional crime and that combatting it requires both innovative law enforcement techniques and new laws designed to address abuses of emerging technologies. In 1984, Congress adopted the latter view and enacted discrete legislation to address crime in electronic environments. Although certain computer crimes appear simply to be old crimes committed in new ways (e.g., the bank teller who uses a computer program to steal money is still committing bank fraud), some computer offenses find their genesis in our new technologies and must be specifically addressed by statute. For example, the widespread damage caused by inserting a virus into a global computer network cannot be prosecuted adequately by relying upon common law criminal mischief statutes. Indeed, it is questionable whether Robert Morris, the individual responsible for launching the Morris worm and crippling 6,000 computers around the world, could have been prosecuted had Congress not had the foresight to enact the Computer Fraud and Abuse Act.

Whether classified as "old" or "new," computer crime creates unique problems for law enforcement and a concomitant threat to the public welfare. The most significant legislative problems stem from technology's shift from a corporeal to an intangible environment. This departure from a physical world (where items are stored in a tangible form that can be carried, such as information written on paper) to an intangible, electronic environment means that computer crimes (and the methods used to investigate them) are no longer subject to traditional rules and constraints. Consider, for example, the way the crimes of theft and criminal mischief have evolved. Before the advent of computer networks, the ability to steal information or damage property was to some extent determined by physical limitations. A burglar could break only so many windows and burglarize only so many homes in a week. During each intrusion, the burglar could carry away only so many items. This does not, of course, make this conduct trivial, but it points out that the amount of property a burglar could steal, or the amount of damage he could cause, had physical limits.

In the information age, of course, these limitations no longer apply. A criminal seeking information stored in a networked computer with dial-in access can acquire that information from virtually anywhere in the world. The quantity of information stolen or the amount of damage caused by malicious programming code may be limited only by the speed of the network and the criminal's computer equipment. Moreover, such conduct can easily occur across state and national borders.

This clear shift to a borderless, incorporeal environment and the increased risk that information will be stolen and transported in electronic form is difficult to address by relying upon older laws written to protect physical property. For example, the statute pertaining to interstate transportation of stolen property, 18 U.S.C. § 2314, speaks of "goods, wares and merchandise," and consequently has been held by at least one court not to apply to intangible property. See United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991). Similarly, the long-familiar extortion statute makes it illegal, in some cases, to threaten physical violence to property. 18 U.S.C. § 1951(a). Although a threat to fire bomb a

building would clearly satisfy this test, a threat to delete files may not.

II. THE STRUCTURE OF TITLE 18 REFORM

There are two ways, conceptually, to address the growing computer crime problem. The first would be to comb through the entire United States Code, identifying and amending every statute potentially affected by the implementation of new computer and telecommunications technologies. The second would be to focus substantive amendments on the Computer Fraud and Abuse Act to specifically address new abuses that spring from the misuse of new technologies.

The new legislation adopts the latter approach for a host of reasons:

(1) The United States, in a single statute, continues to address the core issues driving computer and information security at both domestic and international levels; that is, protecting the confidentiality, integrity, and availability of data and systems. Indeed, these three themes provide the foundation for the Organization for Economic Cooperation and Development's (OECD) Guidelines for the Security of Information Systems. They also serve as the linchpin for emerging domestic works on information privacy. See, e.g., Draft Principles for Providing and Using Personal Information, 60 Fed. Reg. 4362 (January 20, 1995)[hereinafter "Draft Principles"]. By patterning the amended Computer Fraud and Abuse Act on the OECD guidelines, the U.S. is at the forefront of rethinking how information technology crimes must be addressed--simultaneously protecting the confidentiality, integrity, and availability of data and systems. And by choosing this path, we may encourage other countries to adopt a similar framework, thus creating a more uniform approach to addressing computer crime in the existing global information infrastructure.

(2) In most cases, a single point of reference--The Computer Fraud and Abuse Act, 18 U.S.C. § 1030--is provided for investigators, prosecutors, and legislators as they attempt to determine whether a particular abuse of new technology is covered under federal criminal law.

(3) As new technologies are introduced and the criminal law requires reconsideration, fine-tuning § 1030 may well be adequate, and it will not be necessary to continually parse through the entire United States Code.

(4) This statutory scheme will give us a better understanding of the scope of the computer crime problem by enabling more reliable statistics to be generated regarding computer abuse. Under current law, computer crimes can be charged under a host of criminal statutes,

and this situation will continue if the U.S. chooses a patchwork approach and amends the various provisions of Title 18 to address new computer crimes. The existence of various computer crime provisions in different parts of Title 18 exacerbates an already obvious problem; i.e., computer crime experts have long admitted that there are no centralized computer crime statistics, not even within the law enforcement community. Indeed, a June 1996 study by the United States Sentencing Commission concluded that there were only 174 cases in which the statute of conviction included 18 U.S.C. § 1030, but conceded that

> . . .pertinent questions remain unanswered. For example, how much criminal behavior that could have been successfully prosecuted under 18 U.S.C. § 1030 was prosecuted under other fraud statutes. . . ?

United States Sentencing Commission, Report to Congress: Adequacy of Federal Sentencing Guideline Penalties for Computer Fraud and Vandalism Offenses, pp. 2, 6. By centralizing computer crimes under one statute, we may better measure existing harms, anticipate trends, and determine the need for further legislative reform. Additionally, amendments to the sentencing scheme of

18 U.S.C. § 1030 (and the Federal Sentencing Guidelines--2F1.1--upon which actual sentences are based), will be more effectively determined.

(5) Last, 18 U.S.C. § 1030(f) specifically provides that certain government officials, if engaging in lawfully authorized investigative, protective, or intelligence activities, are not restricted by § 1030. By amending only 18 U.S.C. § 1030 to address new high-tech offenses, this exception clearly continues to apply to any newly defined criminal conduct.

III. Specific Amendments: Protecting the Confidentiality, Integrity, and Availability of Systems and Information

A. Section 1030(a)(1)

Title 18, Section 1030(a)(1) originally provided that anyone who knowingly accesses a computer without authorization or exceeds authorized access and obtains 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" is subject to a fine or imprisonment for not more that ten years (for a first offense). 18 U.S.C. § 1030(a)(1)(emphasis added). This scienter element apparently was included when this subsection was originally drafted because it is contained in 18 U.S.C. § 794(a). Section

794(a), however, provides for life imprisonment, whereas § 1030(a)(1) is only a ten-year felony. Therefore, it is more appropriate that the language of § 1030(a)(1) should track 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.

It should be noted that, although there is considerable overlap between § 793(e) and § 1030(a)(1) as amended, the two statutes do not reach exactly the same conduct. Section 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information or restricted data, and subsequently performed some unauthorized communication or other improper act. In this sense then, it is the use of the computer which is being proscribed, not the unauthorized possession of, control over, or subsequent transmission of the information itself. Existing espionage laws would provide an adequate basis for the prosecution of individuals who attempt to peddle governmental secrets to foreign governments. However, a person who deliberately breaks in to a computer for the purpose of obtaining properly classified or restricted information, or attempts to do so, should be subject to criminal prosecution for this conduct.

B. Section 1030(a)(2)

Subsection (a)(2) is, in the truest sense, a provision designed to protect the confidentiality of computer data. As was noted in 1986 by the Senate Judiciary Committee,

> [t]he premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions. . . . Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data.

S. Rep. No. 99-432 at 6.

With the continued evolution of the National Information Infrastructure (NII), however, Congress has come to recognize that not only financial records and credit information warrant federal protection. As noted in the commentary to the Draft Principles, "with the NII, the assumption is that large amounts of sensitive information will be on line, and can be accessed, perhaps without authority, by a large number of network users." 59 Fed. Reg. at 27207. Moreover, "the NII will only achieve its full potential if individual privacy is properly protected." Id. Therefore, the new subsection 1030(a)(2) is designed to insure that

it is punishable to misuse computers to obtain government information and, where appropriate, information held by the private sector. Moreover, the provision has been restructured so that different paragraphs protect different types of information, thus allowing easy additions or modifications to offenses if events require.

Certainly not all computer misuse warrants federal criminal sanctions. The problem is that no litmus test can accurately segregate important from unimportant information, and any legislation may therefore be under- or over-inclusive. For example, a frequent test for determining the appropriateness of federal jurisdiction--a monetary amount--does not work well when protecting information. The theft from a computer of a judge's draft opinion in a sensitive case or the copying of medical records might not meet such a monetary threshold, but clearly such information should be protected. Therefore, the act of taking all of this kind of information is now criminalized. Even so, it is important to remember that the elements of the offense include not just taking the information, but abusing one's computer authorization to do so.

The need to protect information is highlighted by recent studies indicating that people are increasingly misusing computers to obtain information. In 1993, the General Accounting Office (GAO) presented testimony before the House Government Operations Committee, Subcommittee on Information, Justice, Agriculture, and Transportation, on the abuse of National Crime Information Center (NCIC) information. The testimony stated that, following an investigation, GAO determined that (1) NCIC information is valuable, (2) such information has been misused by "insiders" (individuals with authorized access), (3) this misuse included selling NCIC information to outsiders and determining whether friends and relatives had criminal records, and (4) incentives for misuse outweighed potential penalties. Statement of Laurie E. Ekstrand, July 28, 1993, p. 6 [hereinafter "Ekstrand Statement"]. The GAO found that some of this misuse jeopardized the safety of citizens and potentially jeopardized law enforcement personnel. Id. at 16. Moreover, because there were no federal or state laws specifically directed at NCIC misuse, most abusers of NCIC were not criminally prosecuted. Id. at 17. GAO concluded that Congress should enact legislation with strong criminal sanctions specifically directed at the misuse of NCIC. Id. at 20.

Of course, protecting only NCIC data (or, more broadly, criminal history information), would be underinclusive, because other types of sensitive data are clearly at risk. For example, during Operation Desert Storm, it was widely reported that hackers accessed sensitive but unclassified data regarding personnel performance reports, weapons development information, and logistics information regarding the movement of equipment and personnel. Teen tapped computers of U.S. military, Chicago Tribune, November 21, 1991 at 3. NASA computers have also been penetrated, Computer Hacker Charged with Entering NASA System, Washington Post, September 26, 1991 at A20, as have at least two federal courthouse computer systems. See, e.g., U.S. Says Hackers Scanned Data, The New York Times, November 15, 1992, at A40. Some Internal Revenue Service employees also

improperly used IRS computers to examine tax return information. I.R.S. Staff Is Cited in Snoopings, The New York Times, July 19, 1994, at D1, D5.

Clearly, the government should be able to prosecute individuals who obtain government information by misusing computers. Importantly, 18 U.S.C. § 1030(a)(2), as amended, does not punish the mere acquisition of information (which might unduly impede the free flow of ideas), but prohibits intentionally accessing a computer without or in excess of authority and then obtaining such information. Moreover, to the extent that the information obtained is or should be available, it should be obtained through legal means (e.g., public sources or FOIA) and not through hacking.

Subsection 1030(a)(2)(C) is designed to protect against the interstate or foreign theft of information by computer. Such a provision is necessary in light of the Tenth Circuit's decision in United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991), where the court held that purely intangible intellectual property, such as a computer program, cannot constitute goods, wares, merchandise, securities, or moneys which have been stolen, converted, or taken within the meaning of § 2314. "Information" as used in this subsection is meant to be broadly construed and includes information stored in intangible form. Moreover, consistent with Congress's prior construction of § 1030(a)(2), "obtaining information" includes merely reading it; i.e., there is no requirement that the information be copied or transported. This is critically important because, in an electronic environment, information can be "stolen" without asportation, and the original usually remains intact.

Some computers may qualify under more than one subsection of § 1030(a)(2); for example, a particular government computer might be covered by both § 1030(a)(2)(B) and (a)(2)(C). This overlap serves to eliminate legal issues that might have arisen had Congress made the provisions mutually exclusive. Conceivably, in a given case, it may not be clear whether information taken from a government contractor's computer constitutes "information from any department or agency of the United States" under § 1030(a)(2)(B), but the offense might still be chargeable under § 1030(a)(2)(C) if the elements of that subsection are satisfied.

The seriousness of a breach in confidentiality depends, in considerable part, on either the value of the information or the defendant's motive in taking it. Thus, the statutory penalties are structured so that merely obtaining information of minimal value is only a misdemeanor, but certain aggravating factors make the crime a felony. More specifically, the crime becomes a felony if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000.

As for enhancements not based on the value of the property obtained, recent documented

cases indicate that individuals misuse information for a variety of unacceptable purposes. 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 the copyright statute (17 U.S.C. § 506(a)) and wiretap statute (18 U.S.C. § 2511(1)(d)) respectively.

As for the monetary threshold, 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 relationship between the existing § 1030(a)(3) provision and the newly amended § 1030(a)(2) merits some discussion. Section 1030(a)(3) protects the computer from outsiders, even if the hacker obtains no information. Thus, an intruder who violates the integrity of a government machine to gain network access is nonetheless liable for trespass even when he has not jeopardized the confidentiality of data. Section 1030(a)(2), on the other hand, protects the confidentiality of data, even from intentional misuse by insiders. Additionally, although a first violation of § 1030(a)(3) is always a misdemeanor, a § 1030(a)(2) violation may constitute a felony if the information taken is valuable or sufficiently misused. See § 1030(c)(2)(B)(raising the offense to felony level based upon the value or intended use of the improperly acquired data). Although a single act may violate both provisions, the provisions protect against different harms and, in any event, the actor's conduct would be aggregated for the purposes of sentencing.

C. Subsection 1030(a)(3)

Three substantive changes were made to § 1030(a)(3). First, the word "adversely" has been deleted because including this term suggests, inappropriately, that trespassing in a government computer may be benign.

Second, for clarity, the term "the use of the Government's operation of such computer" has been replaced with the term "that use by or for the Government of the United States." When a computer is used for the government, the government is not necessarily the operator, and the old term may have led to confusion. Consistent with this change, a similar change was made to the definition of "federal interest computer" (redesignated as "protected computer") in § 1030(e)(2)(A). Third, Congress inserted "non-public" to modify "computer of a department or agency of the United States." This change is intended to reflect the growing use of the Internet by government agencies and, in particular, the establishment of World Wide Web home pages and other public services. Arguably, a person charged under the old subsection (a)(3) might have asserted as a defense that he was not "without authorization to access any computer of a department or agency of the United States," because he was authorized to access some publicly available computer of that department or agency, such as

a Web site. While this defense would almost have negated the law and thus defied a common-sense interpretation of the former law, Congress added the word "non-public" to make it perfectly clear that a person who has no authority to access any non-public computer of a department or agency may be convicted under (a)(3) even though permitted to access publicly available computers.

D. Subsection 1030(a)(4)

Subsection 1030(a)(4) has been amended to insure that felony level sanctions apply when unauthorized use of the computer (or use exceeding authorization) is significant. At the time the "computer use" exception was originally crafted, the Senate Judiciary Committee noted that:

> [T]he mere use of a computer or computer service has a value all its own. Mere trespasses onto someone else's computer system can cost the system provider a "port" or access channel that he might otherwise be making available for a fee to an authorized user. At the same time, the Committee believes it is important to distinguish clearly between acts of fraud under (a)(4), punishable as felonies, and acts of simple trespass, punishable in the first instance as misdemeanors. That distinction would be wiped out were the Committee to treat every trespass as an attempt to defraud a service provider of computer time.

S. Rep. No. 99-432, 99th Cong., 2d Sess. 10 (1986). See also H.R. Rep. No. 99-612, 99th Cong., 2d Sess. 12 (1986).

Although Congress retains the concern about converting every trespass into a felony scheme to defraud, this new amendment clearly recognizes that a blanket exception for computer use may be too broad. Hackers, for example, have broken into Cray supercomputers for the purpose of running password cracking programs, sometimes amassing computer time worth far in excess of $5,000. In light of the large expense to the victim caused by some of these trespassing incidents, it is more appropriate to except from the felony provisions of subsection 1030(a)(4) only cases involving no more than $5,000 of computer use during any one-year period.

E. Subsection 1030(a)(5)

Subsection 1030(a)(5) was completely restructured in 1994, but the 1994 law may have had some unintended consequences. Most notably, certain government and financial institution computers may have been denied previously existing federal protection; some hacking activities may have been inappropriately decriminalized; and certain insider conduct may

have been inappropriately criminalized.

In the 1994 amendments, the reach of this subsection was broadened by replacing the term "federal interest computer" with the term "computer used in interstate commerce or communications." The latter term is broader because the old definition of "federal interest computer" in 18 U.S.C. § 1030(e)(2)(B) covered a computer "which is one of two or more computers used in committing the offense, not all of which are located in the same State." This meant that a hacker who attacked other computers in the same state was not subject to federal jurisdiction, even when these actions may have severely affected interstate or foreign commerce. For example, individuals who attack telephone switches may disrupt interstate and foreign calls. The 1994 change remedied that defect.

However, the definition of federal interest computer actually covered more than simply interstate activity. More specifically, 18 U.S.C. § 1030(e)(2)(A) covered, generically, computers belonging to the United States Government or financial institutions, or those used by such entities on a non-exclusive basis if the conduct constituting the offense affected the Government's operation or the financial institution's operation of such computer. By changing § 1030(a)(5) from "federal interest computer" to "computer used in interstate commerce or communications," Congress may have inadvertently eliminated federal protection for those government and financial institution computers not used in interstate communications. For example, the integrity and availability of classified information contained in an intrastate local area network may not have been protected under the 1994 version of 18 U.S.C. § 1030(a)(5), although its confidentiality continued to be protected under

18 U.S.C. § 1030(a)(1). To remedy this situation in the 1996 Act, 18 U.S.C. § 1030(a)(5) was redrafted to cover any "protected computer," a new term defined in § 1030(e)(2) and used throughout the new statute--in § 1030(a)(5), as well as in §§ 1030(a)(2), (a)(4), and the new (a)(7). The definition of "protected computer" includes government computers, financial institution computers, and any computer "which is used in interstate or foreign commerce or communications."

This broad definition addresses the original concerns regarding intrastate "phone phreakers" (i.e., hackers who penetrate telecommunications computers). It also specifically includes those computers used in "foreign" communications. With the continually expanding global information infrastructure, with numerous instances of international hacking, and with the growing possibility of increased global industrial espionage, it is important that the United States have jurisdiction over international computer crime cases. Arguably, the old definition of "federal interest computer" contained in 18 U.S.C. § 1030(e)(2) conferred such jurisdiction because the requirement that the computers used in committing the offense not all be located in the same state might be satisfied if one computer were located overseas. As

a general rule, however, Congress's laws have been presumed to be domestic in scope only, absent a specific grant of extraterritorial jurisdiction. E.E.O.C. v. Arabian American Oil Co., 499 U.S. 244 (1991). To ensure clarity, the statute was amended to reference international communications explicitly.

Another concern with the 1994 version of 18 U.S.C. § 1030(a)(5) involved the overall statutory scheme. Under the 1986 version of subsection 1030(a)(5), the actor causing the harm must have been without authority to access the victim computer. As such, the provision never applied to insiders, although insiders are often responsible for intentionally causing computer damage. Indeed, the Justice Department was forced to decline prosecution in some cases where individuals intentionally inserted malicious programming code into computers, because those individuals were authorized to access the attacked system. The 1994 law, in contrast to the 1986 version, appropriately applied to both insiders and those without authorized access who intentionally caused damage.

Unfortunately, however, by eliminating the trespassing requirement, and at the same time requiring the government to prove that the actor either intentionally or recklessly caused damage, the 1994 law no longer punished a person who broke into a federal interest computer and "thereby caused loss." See

18 U.S.C. § 1030(a)(5)[1986 version]. Thus, the enactment of the 1994 legislation decriminalized some hacking and inadvertently sent the message that breaking into computers was acceptable so long as the actor neither intended nor recklessly caused damage. However, in these 1996 amendments, criminal liability for such behavior has been restored. This was clearly necessary in light of the increased importance of computer networks in today's society and the nation's considerable interest in creating a trusted national information infrastructure that insures the confidentiality, integrity, and availability of information and systems.

This problem, now corrected, arose because the 1986 and 1994 versions of section 1030(a)(5) defined improper conduct in completely different ways--the former by focusing only on the actor's authority to access the computer; the latter by considering solely the actor's intent. Of course, these two separate litmus tests each cover important aspects of criminal computer damage, but neither measure, taken alone, fully succeeds in describing the acts which should be criminal. For example, although those who intentionally damage a system should be punished regardless of whether they are authorized users, it is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional. In such cases, it is the intentional act of trespass that makes the conduct criminal. To provide otherwise is to openly invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause, they commit no crime unless that damage was either intentional or reckless. Rather then send such a dangerous

message (and deny victims any relief), it is better to insure that § 1030(a)(5) criminalizes all computer damage done by outsiders, as well as intentional damage by insiders, albeit at different levels of severity.

By using a matrix, it is easy to see that neither the 1986 law nor the 1994 law was adequate, although they fail in different categories.

MATRIX 1: § 1030(a)(5)[1986 Version]
[Based on the defendant's authority to access the computer]

	Trespassers	**Authorized Users**
Intentional Damage	Felony	No crime
Reckless Damage	Felony	No crime
Negligent Damage	Felony	No crime

MATRIX 2: 18 U.S.C. § 1030(a)(5)[1994 Version]
[Based on the defendant's criminal intent to damage]

	Trespassers	**Authorized Users**
Intentional Damage	Felony	Felony
Reckless Damage	Misdemeanor	Misdemeanor
Negligent Damage	No crime	No crime

Conceptually, a comprehensive statutory scheme does not treat these two tests--mental state and authority to access--as mutually exclusive. Instead, it integrates them to cover all kinds of serious misconduct. Just as important, it recognizes that some behaviors are less serious, or should not be criminal offenses at all. For example, the 1994 law created a misdemeanor for reckless damage without distinguishing between trespassers and authorized users.

Whether authorized users should ever be criminally liable for reckless damage is a debatable question. For example, it could be deemed reckless in today's computer environment to intentionally copy a file from a floppy diskette to a hard drive without first running a virus scan--although imposing criminal sanctions for such conduct is clearly inappropriate, absent other evidence of criminal intent. On the other hand, reckless trespassers warrant felony prosecutions, since they are unauthorized users who pose significant risks to computer systems. Thus, Congress has now chosen an approach that integrates access and authority tests in the following way:

MATRIX 3: 18 U.S.C. § 1030(a)(5) [THE NEW LAW]

[Based on the defendant's authority to access the computer and criminal intent to damage]

	Trespassers	**Authorized Users**
Intentional Damage	Felony	Felony
Reckless Damage	Felony	No crime
Negligent Damage	Misdemeanor	No crime

Essentially, this new statute provides that individuals who access protected computers without authority are responsible for the consequences of their actions, but those accessing with authority are criminally liable only if they intend to cause damage to the victim.

Although subsections § 1030(a)(5)(B) and (a)(5)(C) require that the actor cause damage as a result of his or her unauthorized access, damages are not limited to those caused by the process of gaining illegal entry. Rather, all damage, whether caused while gaining access or after entry, is relevant.

Another concern with the 1994 law was that it required both "damage" and "loss," without clearly articulating what constituted "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers 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 nor its information has been damaged. Nonetheless, the intruder's conduct allowed him to accumulate valid user passwords to the system, required all system users to change their passwords, and required the system administrator to devote resources to re-securing the system. Thus, although there may be no permanent "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.

It would not have been possible to address all of these concerns by making only minor amendments to subsection 1030(a)(5). Thus, the statutory scheme was altered to both simplify its provisions and adopt the sanctions provided in Matrix 3.

As discussed further below, the term "damage" remains, but is now defined in 18 U.S.C. § 1030(e)(8). Consistent with the view that § 1030(a)(5) protects the integrity and availability of data and systems, "damage" means any impairment of those attributes. The statutory language avoids listing specific acts that can cause such impairment to insure that its coverage is suitably broad. For example, in the 1986 version, the terms "alters, damages or destroys information," were included, inadvertently raising new issues (e.g., whether encrypting data satisfies this test since the underlying original information remains unchanged). Rather than providing a list of prohibited actions and risk being underinclusive, the statute focuses instead on the harms it seeks to prevent.

This harm-based definition of "damage" can now be found in subsections 1030(e)(8)(A) through (D). As in the past, the term "damage" will require meeting one of several significant thresholds. Two of these measures survive from earlier versions of § 1030: the first is significant financial losses--although raised in these amendments from $1000 to $5000--[§ 1030(e)(8)(A)]; the second is potential impact on medical treatment [§ 1030(e)(8)(B)]. In addition, Congress has listed two new threshold harms in its definition of "damage": causing physical injury to any person [18 U.S.C. § 1030(e)(8)(c)] and threatening the public health or safety [18 U.S.C. § 1030(e)(8)(c)]. As the NII and other network infrastructures continue to grow, computers will increasingly be used for access to critical services such as emergency response systems and air traffic control, and will be critical to other systems that we cannot yet anticipate. Thus, any definition of "damage" must broadly encompass the types of harms against which people should be protected.

Having amended the structure of § 1030(a)(5), Congress needed to amend the civil penalty provision under § 1030(g). The subsection as amended provides that victims of computer abuse can maintain a civil action against the violator to obtain compensatory damages, injunctive relief, or other equitable relief, but damages are limited to economic damages for cases where the only damage suffered by the plaintiff is monetary loss as defined by § 1030(e)(8)(A).

F. Subsection 1030(a)(7)

New subsection (a)(7) is designed to respond to a growing problem: the interstate transmission of threats directed against computers and computer networks. Such threats, if

accompanied by an intent to extort, may already be covered in some instances by the Hobbs Act, 18 U.S.C. § 1951, which applies to interference with commerce by extortion. They also may be covered in some instances by 18 U.S.C. § 875(d), which applies to interstate communication of a threat to injure the property of another. However, under both of these statutes, it is not absolutely clear that "property" includes the unimpaired operation of a computer or the unrestricted access to the data or programs stored in a computer and its peripheral equipment. Moreover, it is not clear that certain actions (such as encrypting someone's data and then demanding money for the key) constitute a threat to "injure the property of. . .another." See 18 U.S.C. § 875(d).

These concerns are not theoretical. In one recent case, for example, an individual threatened to crash a computer system unless he was granted access to the system and given an account. Another case involved an individual who penetrated a city government's computer system and encrypted the data on a hard drive, thus leading the victim to suspect an extortion demand was imminent. (This demand never came, however, and fortunately the victim was able to recover from the incident.) Although the number of such incidents is currently small, the explosion in network access has substantially increased the risk that such conduct will occur, and our nation's increased reliance on computers clearly suggests that such activities, if not deterred, will severely impair our ability to use the NII effectively. Moreover, since such extortion and threats will normally involve interstate and foreign communications, federal law enforcement needed a clear basis to address this new problem quickly.

It is worth noting that subsection (a)(7) covers any interstate or international transmission of threats against computers, computer networks, and their data and programs, whether the threat is received by mail, a telephone call, electronic mail, or through a computerized message service. The provision is worded broadly to cover threats to interfere in any way with the normal operation of the computer or system in question, such as denying access to authorized users, erasing or corrupting data or programs, or slowing down the operation of the computer or system. The extortion element is modeled after that in 18 U.S.C. §§ 875(b) and (d).

G. Sentencing Provisions: Subsection 1030(c)

The sentencing provisions of § 1030 have been altered to reflect the new statutory scheme and to address an old, technical error. As previously enacted, recidivists were only subject to enhanced penalties if they violated the same subsection twice. For example, if an individual violated the Act by committing fraud by computer [subsection (a)(4)] and later committed another computer crime offense by intentionally destroying medical records [subsection (a)(5)], he was not a recidivist because his conduct violated two separate subsections of § 1030. Congress has changed the statutory language to provide that anyone who is convicted

twice of committing a computer offense will be subjected to enhanced penalties.

H. Jurisdiction: Subsection 1030(d)

Having created several new crimes in 18 U.S.C. § 1030, Congress needed to consider the jurisdictional grant in 18 U.S.C. § 1030(d). For some time, the Federal Bureau of Investigation and the United States Secret Service have shared concurrent jurisdiction over § 1030 based upon a Memorandum of Understanding. This new Act, by creating certain new crimes, does not alter any existing agreements, nor limit or alter an agency's "traditional" jurisdiction. Thus, there is new language in 18 U.S.C. § 1030(d) to insure that the status quo is maintained. For example, the new 18 U.S.C. § 1030(a)(2)(C) addressed gaps in 18 U.S.C. § 2314 (interstate transportation of stolen property), and the new 18 U.S.C. § 1030(a)(7) addressed gaps in 18 U.S.C. § 1951 (the Hobbs Act) and 18 U.S.C. § 875 (interstate communications). All of these statutes are within the traditional jurisdiction of the FBI, therefore 18 U.S.C. § 1030(d) did not extend to the United States Secret Service concurrent jurisdiction over these types of offenses, even when committed by computer. Subsections over which the Secret Service maintains concurrent jurisdiction are § 1030(a)(2)(A) and (B), (a)(3), (a)(4), (a)(5), and (a)(6).

Updated June 10 ,1998

usdoj-crm/mis/mdf
