Order Code 97-1025

CRS Report for Congress
Received through the CRS Web

Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws

Updated June 28, 2005

Charles Doyle
Senior Specialist
American Law Division

Alyssa Bartlett Weir
Law Clerk
American Law Division

Penny Hill Press
http://www.crsdocuments.com
GalleryWatch.com

Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws

Summary

The federal computer fraud and abuse statute, 18 U.S.C. 1030, protects federal computers, bank computers, and computers used in interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills crack and gaps in the protection afforded by other federal criminal laws. This is a brief sketch of section 1030 and some of its federal statutory companions.

In their present form, the seven paragraphs of subsection 1030(a) outlaw:

- computer trespassing (e.g., hacking) in a government computer, 18 U.S.C. 1030(a)(3);
- computer trespassing (e.g., hackers) resulting in exposure to certain governmental, credit, financial, or commercial information, 18 U.S.C. 1030(a)(2);
- damaging a government computer, a bank computer, or a computer used in interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, a denial of service attack, and other forms of cyber attack, cyber crime, or cyber terrorism), 18 U.S.C. 1030(a)(5);
- committing fraud an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030(a)(4);
- threatening to damage a government computer, a bank computer, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030(a)(7);
- trafficking in passwords for a government computer, a bank computer, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030(a)(6); and
- accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1).

Subsection 1030(b) makes it a crime to attempt to commit any of these offenses. Subsection 1030(c) catalogs the penalties for committing them, penalties that range from imprisonment for not more than a year for simple cyberspace trespassing to a maximum of life imprisonment when death results from intentional computer damage. Subsection 1030(d) preserves the investigative authority of the Secret Service. Subsection 1030(e) supplies common definitions. Subsection 1030(f) disclaims any application to otherwise permissible law enforcement activities. Subsection 1030(g) creates a civil cause of action of victims of these crimes.

Earlier versions of this report appeared under the title, *Computer Fraud and Abuse: An Overview of 18 U.S.C. 1030 and Related Federal Criminal Laws.*

Contents

Introduction 1
Trespassing in Government Cyberspace
- 18 U.S.C. 1030(a)(3) 3
- Intent 4
- Jurisdiction 4
- Unauthorized Access 5
- Affects the Use 6
- Penalties 6
- Other Crimes 10

Obtaining Information
by Unauthorized Computer Access
- 18 U.S.C. 1030(a)(2) 16
- Jurisdiction 18
- Intent 19
- Penalties 19
- Other Crimes 21

Causing Computer Damage
- 18 U.S.C. 1030(a)(5) 23
- Intent 24
- Damage 24
- Jurisdiction 27
- Penalties 29
- Other Crimes 31

Computer Fraud
- 18 U.S.C. 1030(a)(4) 42
- Jurisdiction 42
- Intent 43
- Penalties 44
- Other Crimes 45

Extortionate Threats
- 18 U.S.C. 1030(a)(7) 72
- Jurisdiction 73
- Threat of “damage” 73
- Intent 74
- Threats 74
- Penalties 75
- Other crimes 76

Trafficking in Computer Access 18 U.S.C. 1030(a)(6) 79
- Jurisdiction 80
- Intent 80
- Penalties 80
- Other crimes 81

Computer Espionage
- 18 U.S.C. 1030(a)(1) 81
- Jurisdiction 83
- Intent 83
- Penalties 83
- Other crimes 84

APPENDIX 88
Selected Bibliography 88
18 U.S.C. 1030 89

Penny Hill Press
http://www.crsdocuments.com
GalleryWatch.com™

Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws

Introduction

The federal computer fraud and abuse statute, 18 U.S.C. 1030,[1] protects computers in which there is a federal interest – federal computers, bank computers, and computers used in interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, instead it fills cracks and gaps in the protection afforded by other state and federal criminal laws. It is a work that over the last two decades, Congress has kneaded, reworked, recast, and amended to bolster the uncertain coverage of more general federal trespassing, threat, malicious mischief, fraud, and espionage statutes.[2] This is a brief description of section 1030 and its federal statutory companions.

---

[1] The full text of 18 U.S.C. 1030 is appended.

[2] Congressional inquiry began no later than 1976, S. Comm. on Government Operations, *Problems Associated with Computer Technology in Federal Programs and Private Industry – Computer Abuses*, 94th Cong., 2d Sess. (1976)(Comm.Print). Hearings were held in successive Congresses thereafter until passage of the original version of section 1030 as part of the Comprehensive Crime Control Act of 1984, Pub.L.No. 98-473, 98 Stat. 2190; *see e.g.*, *Federal Computer Systems Protection Act: Hearings Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess.(1978); *S.240, the Computer Systems Protection Act of 1979: Hearings Before the Subcomm. on Criminal Justice of the Senate Comm. on the Judiciary*, 96th Cong., 2d Sess.(1980); *Federal Computer System Protection Act, H.R. 3970: Hearings Before the House Comm. on the Judiciary*, 97th Cong., 2d Sess.(1982); *Computer Crime: Hearings Before the House Comm. on the Judiciary*, 98th Cong., 1st Sess. (1983).

Refurbishing of the original 1984 legislation occurred in 1986, 1988, 1989, 1990, 1994, and 1996: Pub.L.No. 99-474, 100 Stat. 1213; Pub.L.No. 100-690, 102 Stat. 4404; Pub.L.No. 101-73, 103 Stat. 502; Pub.L.No. 101-647, 104 Stat. 4831; Pub.L.No. 103-322, 108 Stat. 2097; Pub.L.No. 104-294, 110 Stat. 3491. Most recently, both the USA PATRIOT Act, Pub.L.No. 107-56, 115 Stat. 272 (2001) and the Department of Homeland Security Act, Pub.L.No. 107-296, 116 Stat. 72135 (2002) amended provisions of section 1030.

For a chronological history of the Act up to but not including the 1996 amendments, see Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECHNOLOGY LAW JOURNAL 403 (1996). For a general description of the validity and application of this Act, see Buchman, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 ALR Fed. 101 (2004); Berkowitz, *Computer Security and Privacy: The Third Wave of Property Law*, 33 COLORADO LAWYER 57 (Feb. 2004).

There are other laws that address the subject of crime and computers. Section 1030 deals with computers as victims; other laws deal with computers as arenas for crime or as repositories of the evidence of crime or from some other perspective. These other laws – laws that are about things like encryption, obscenity, pornography, and gambling – are beyond the scope of this report.[3]

In their present form, the seven paragraphs of subsection 1030(a) outlaw:

- computer trespassing in a government computer, 18 U.S.C. 1030(a)(3);
- computer trespassing resulting in exposure to certain governmental, credit, financial, or commercial information, 18 U.S.C. 1030(a)(2);
- damaging a government computer, a bank computer, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030(a)(5);
- committing fraud an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030(a)(4);
- threatening to damage a government computer, a bank computer, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030(a)(7);
- trafficking in passwords for a government computer, a bank computer, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030(a)(6); and
- accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1).

Subsection 1030(b) makes it a crime to attempt to commit any of these offenses.[4] Subsection 1030(c) catalogs the penalties for committing them, penalties

---

[3] For a discussion of these and similar matters see, *Nineteenth Survey of White Collar Crime: Computer Crimes*, 41 AMERICAN CRIMINAL LAW REVIEW 313 (2004); Cohen, *Obscenity and Indecency: Constitutional Principles and Federal Statutes*, CRS REP. 95-804 (Jan. 3, 2005); Cohen, *Child Pornography: Constitutional Principles and Federal Statutes*, CRS REP. 95-406 (Oct.15, 2003); Wilson, *Computer Attack and Cyber Terrorism*, CRS REP. RL32114 (Apr. 1 2005); Grimmett, *Encryption Export Controls*, CRS REP. RL30273 (Jan.11, 2001); *Casting a Net Over the Net: Attempts to Protect Children in Cyberspace*, SETON HALL CONSTITUTIONAL LAW JOURNAL 1123 (2000); Doyle, *Internet Gambling: Overview of Federal Criminal Law*, CRS REP. No. 97-619 (Nov. 29, 2004); Kerr, *Search and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE (July, 2002), on www.cybercrime.gov (June 16, 2005).

[4] The Department of Justice maintains a website at <http://www.cybercrime.gov/cccases.html> which provides a list of all prosecutions for "computer intrusion", commonly known as "hacking,"as well as cases, statutes and other

that range from imprisonment for not more than a year for simple cyberspace trespassing to imprisonment for not more than twenty years for a second espionage-related conviction. Subsection 1030(d) preserves the investigative authority of the Secret Service. Subsection 1030(e) supplies common definitions. Subsection 1030(f) disclaims any application to otherwise permissible law enforcement activities. Subsection 1030(g) creates a civil cause of action for victims of these crimes. And subsection 1030(h) called for annual reports through 1999 from the Attorney General and Secretary of the Treasury on investigations under the damage paragraph (18 U.S.C. 1030(a)(5)).

Trespassing in Government Cyberspace 18 U.S.C. 1030(a)(3)

> *Whoever . . . intentionally, without authorization to access any nonpublic computer*[5] *of a department or agency of the United States,*[6] *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.*
> *(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.*

Paragraph 1030(a)(3) condemns unauthorized intrusion ("hacking") into federal government computers whether they are used exclusively by the government or the government shares access with others. With the help of subsection 1030(b) it also outlaws attempted intrusions. In the case of shared computers, a crime only occurs if the unauthorized access "affects . . . use by or for" the government or would affect such use if an attempted effort had succeeded.[7]

---

documentation associated with cybercrime. The site notes that many of the cases listed therein were based upon section 1030.

[5] "(e) As used in this section . . . (1) the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device," 18 U.S.C. 1030(e)(1).

[6] "(e) As used in this section . . .(7) the term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5," 18 U.S.C. 1030(e)(7).

[7] Broken down into its elements, paragraph (a)(3) makes it unlawful for anyone to:

- without authorization
- intentionally
- either
  - access a government computer maintained exclusively for the use of the federal government, or
  - access a government computer used, at least in part, by or for the federal government and the access affects use by or for the federal government, or
  - attempt to do so (18 U.S.C. 1030(b)).

This pure trespassing proscription dates from 1986 and its legislative history leaves little doubt that nothing more than unauthorized entry is required:

> "[S]ection 2(b) will clarify the present 18 U.S.C. 1030(a)(3), making clear that it applies to acts of simple trespass against computers belonging to, or being used by or for, the Federal Government. The Department of Justice and others have expressed concerns about whether the present subsection covers acts of mere trespass, i.e., unauthorized access, or whether it requires a further showing that the information perused was 'used, modified, destroyed, or disclosed.' To alleviate those concerns, the Committee wants to make clear that the new subsection will be a simple trespass offense, applicable to persons without authorized access to Federal computers," S.Rep.No. 99-432 at 7 (1986); see also, H.R.Rep.No. 99-612 at 11 (1986).

Intent.

The paragraph only bans "intentional" trespassing. The reports are instructive here, for they make it apparent that the element cannot be satisfied by a mere inadvertent trespass and nothing more. It contemplates those who purposefully accomplish the proscribed unauthorized entry into a government computer, and, at least in the view of the House report, those "whose initial access was inadvertent but who then deliberatively maintains access after a non-intentional initial contact," H.R.Rep. No. 99-612 at 9-10 (1986); see also, S.Rep.No. 99-432 at 5-6 (1986).

Jurisdiction.

The reports offer little insight into the meaning of the third element – what computers are protected from trespassing. There may be two reasons. Paragraph 1030(a)(3) protects only government computers and therefore explanations of the sweep of its coverage in the area of interstate commerce or of financial institutions are unnecessary. Besides, at least for purposes of these trespassing offenses of paragraph 1030(a)(3), the statute itself addresses several of the potentially more nettlesome questions.

First, the construction of the statute itself strongly suggests that it reaches only computers owned or leased by the federal government: "whoever . . . 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*. . . ."

Second, the language of the statute indicates that "nonpublic" computers may nevertheless include government computers that the government allows to be used by nongovernmental purposes: "in the case of *a [government] computer not exclusively for the use of the Government of the United States* . . . ."

Third, the statute covers government computers that are available to nongovernment users: "accesses such a computer . . . that . . . in the case of a [government] computer not exclusively for the use of the Government of the United States, is used by *or for* the Government of the United States . . . ." The use of the term "nonpublic," however, makes it clear that this shared access may not be so broad as to include the general public.

Finally, the section supplies a definition of "department of the United States": "[a]s used in this section . . . the term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5," 18 U.S.C. 1030(e) (7);[8] and the title supplies a definition of "agency of the United States": "[a]s used in this title . . .[t]he term 'agency' includes any department, independent establishment, commission, administration, authority, board or bureau of the United States or any corporation in which the United States has a proprietary interest, unless the context shows that such term was intended to be used in a more limited sense," 18 U.S.C. 6.

Unauthorized Access.

While the question of what constitutes "access without authorization" might seem fairly straight forward, Congress was willing to accept a certain degree of trespassing by government employees in order to protect whistleblowers:

> The Committee wishes to be very precise about who may be prosecuted under the new subsection (a)(3). The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would not face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct. At the same time, the Committee was required to balance its concern for Federal employees and other authorized users against the legitimate need to protect Government computers against abuse by "outsiders." The Committee struck that balance in the following manner.
>
> In the first place, the Committee has declined to criminalize acts in which the offending employee merely 'exceeds authorized access' to computers in his own department ("department"' is defined in section 2(g) of S.2281 [now 18 U.S.C. 1030(e)(7)]). It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at. This is especially true where the department in question lacks a clear method of delineating which individuals are authorized to access certain of its data. The Committee believes that administrative sanctions are more appropriate than criminal punishment in such a case. The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers – no matter how slightly – he could be prosecuted under this subsection. That danger will be prevented by not including "exceeds authorized access" as part of this subsection's offense.
> In the second place, the Committee has distinguished between acts of unauthorized access that occur within a department and those that involve trespasses into computers belonging to another department. The former are not covered by subsection (a)(3); the latter are. Again, it is not difficult to envision

---

[8] "The Executive Departments are: the Department of State; the Department of the Treasury; the Department of Defense; the Department of Justice; the Department of the Interior; the Department of Agriculture; the Department of Commerce; the Department of Labor; the Department of Health and Human Services; the Department of Housing and Urban Development; the Department of Transportation; the Department of Energy; the Department of Education; [and] the Department of Veterans Affairs," 5 U.S.C. 101.

> an individual who, while authorized to use certain computers in one department, is not authorized to use them all. The danger existed that S.2281, as originally introduced, might cover every employee who happens to sit down, within his department, at a computer terminal which he is not officially authorized to use. These acts can also be best handled by administrative sanctions, rather than by criminal punishment. To that end, the Committee has constructed its amended version of (a)(3) to prevent prosecution of those who, while authorized to use some computers in their department, use others for which they lack the proper authorization. By precluding liability in purely 'insider' cases such as these, the Committee also seeks to alleviate concerns by Senators Mathias and Leahy that the existing statute cases a wide net over "whistleblowers". . . .
>
> The Committee has thus limited 18 U.S.C. 1030(a)(3) to cases where the offender is completely outside the Government, and has no authority to access a computer of any agency or department of the United States, or where the offender's act of trespass is interdepartmental in nature. The Committee does not intend to preclude prosecution under this subsection if, for example, a Labor Department employee authorized to use Labor's computers accesses without authorization an FBI computer. An employee who uses his department's computer and, without authorization, forages into data belonging to another department is engaged in conduct directly analogous to an 'outsider' tampering with Government computers. . . .
>
> The Committee acknowledges that in rare circumstances this may leave serious cases of intradepartmental trespass free from criminal prosecution under (a)(3). However, the Committee notes that such serious acts may be subject to other criminal penalties if, for example, they violate trade secrets laws or 18 U.S.C. 1030(a)(1), (a)(4), (a)(5), or (a)(6), as proposed in this legislation. S.Rep.No. 99-432 at 7-8 (1986); see also, H.R.Rep.No. 99-612 at 11 (1986).

Affects the Use.

Trespassing upon governmental computer space on computers that are not exclusive for governmental use is prohibited only when it affects use by the government or use for governmental purposes. The committee reports provide a useful explanation of the distinctive, "affects-the-use" element of the trespassing ban:

> [T]respassing in a computer used only part-time by the Federal Government need not be shown to have affected the operation of the government as a whole. The Department of Justice has expressed concerns that the present subsection's language could be construed to require a showing that the offender's conduct would be an exceedingly difficult task for Federal prosecutors. Accordingly, Section 2(b) will make clear that the offender's conduct need only affect the use of the Government's operation of the computer in question [or the operation of the computer in question on behalf of the Government]. S.Rep.No.99-432 at 6-7 (1986); see also, H.R.Rep.No. 99-612 at 11 (1986); S.Rep.No. 104-357 at 9 (1996).

Penalties.

The penalties for violation or attempted violation of paragraph 1030(a)(3) imprisonment for not more than one year and/or a fine of not more than $100,000

($200,000 for organizations) for the first offense and imprisonment for not more than ten years and/or a fine of not more than $250,000 ($500,000 for organizations) for all subsequent convictions, 18 U.S.C. 1030(c), 3571.[9] The Sentencing Guidelines treat violations of paragraph 1030(a)(3) as a trespass, U.S.S.G. §2B2.3, and as a general rule punishable by imprisonment for no more than one year (base offense level 4), even in the case of a second offender, unless the crime involves related but uncharged damage or other aggravating factors.[10] If the offense involves a computer system used as part of the critical infrastructure[11] or by or for a government entity for

---

[9] By virtue of 18 U.S.C. 3571, all felonies are subject to fines of not more than the greater of $250,000 or twice the amount of the pecuniary gain or loss associated with the offense, unless provisions applicable to a specific crime either call for a higher maximum fine or were enacted subsequent to 1984 when the general provisions of section 3571 became effective.

Most federal criminal statutes give the impression that offenders may be sentenced to imprisonment, to a fine or to both imprisonment and a fine. This may be something of an illusion in most serious federal cases. Federal sentencing is governed by sentencing guidelines that calibrate sentencing levels beneath the maximum terms established in the statute for a particular offense, according to the circumstances of the crime and the offender, see generally, Doyle, *How the Federal Sentencing Guidelines Work: Two Examples*, CRS REP. RL32846 (April 4, 2005). As a practical matter, the guidelines call for a term of imprisonment for almost any felony that carries a maximum term of imprisonment of "not more than 10 years" or higher and many that carry a maximum of term of imprisonment of "not more than 5 years." In *United States v. Booker*, 125 S. Ct. 738 (2005), the federal sentencing guidelines were rendered advisory by the Supreme Court because of Sixth Amendment concerns regarding the right to a jury trial and the standard of review on appeal in relation to the mandatory nature of the guidelines, thus "[t]he Act cannot remain valid in its entirety. Severance and excision are necessary." Id. 744.

[10] The Guidelines provide for a number of circumstances under which the base offense level assigned to a particular offense might be raised or lowered. For instance, offenders with sophisticated hacking skills may be subject to the addition of further offense levels as a consequence of the special skill adjustment dictated by the guidelines, U.S.S.G. §3B1.3; *United States v. Petersen*, 98 F.3d 502, 506-8 (9th Cir. 1996)(upholding an upward adjustment to the otherwise applicable guideline range for a defendant who in violation of paragraph 1030(a)(4)(fraud) had hacked into a radio station's computer and managed to successfully rig its promotional contests so as to defraud the station of $40,000 in cash prizes; two Porsche automobiles; and two trips to Hawaii, and who had nearly been successful in executing a $150,000 wire transfer from a financial institution again in violation of paragraph 1030(a)(4)). But see, *United States v. Lee,* 296 F.3d 792 (2002)(court finding that sentencing enhancement because of special skills was unwarranted because there was no showing that "the computer skills used by defendant required substantial education, training, or licensing"). Moreover, the Guidelines allow for uncharged but related conduct. Thus, even though an offender might be charged only under paragraph (a)(3)(simple hacking) if the offense in fact results in damage, the applicable sentencing range is increased to account for the amount of damage done, U.S.S.G. §§2B2.3(b)(3), 2B1.1.

[11] The Guidelines define "critical infrastructure" as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and

purposes of national security, national defense, or the administration of justice, then the Guidelines increase the base offense level to 6 (yielding a sentencing range of no more than a year and a half), again even in the case of a second offender but subject to adjustments for uncharged damage or other aggravating factors.

Any property derived from a violation of 1030 is subject to confiscation by federal authorities who may proceed under either civil or criminal forfeiture procedures.[12] Offenders are also subject to civil liability for any "person" who suffers "damage or loss" may sue for compensatory damages and/or injunctive relief, 18 U.S.C. 1030(g).[13] Offenders may also be subject to a restitution order.[14]

---

rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public," U.S.S.G. §2B2.3, *Application Note* 1. Thus, computers used to maintain or operate a "critical infrastructure" in many, if not most, instances will not be federal or federal use computers and thus not come under the protection of paragraph 1030(a)(3).

[12] Civil forfeiture proceedings are conducted *in rem* against the "offending" property, 18 U.S.C. 981(a)(1)(C)("(a)(1) The following property is subject to forfeiture to the United States . . . (C) Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of section . . . 1030 . . . of this title"); criminal forfeiture occurs as a consequence of the offender's criminal conviction, 18 U.S.C. 982(a)(2)(B)("The court, in imposing sentence on a person convicted of an offense in violation of, or a conspiracy to violate . . . (B) section 1030 of this title, shall order that the person forfeit to the United States any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation").

[13] "(g) Any person [*i.e.*,any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity] who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware," 18 U.S.C. 1030(g), (e)(12).

Although subsection 1030(g) applies to any violations under any of the paragraphs of section 1030, it is discussed at greater length below in connection with paragraph 1030(a)(5)(relating to inflicting damage upon a computer).

[14] 18 U.S.C. 3663; *United States v. Dickerson*, 370 F.3d 1330 (11th Cir. 2004) (court ordered defendant convicted of wire fraud to pay restitution to the Social Security Administration); *cf., United States v. Harris*, 302 F.3d 72 (2d Cir. 2002).

Paragraph 1030(a)(3) has remained essentially unchanged since 1986,[15] and there appear to have been relatively few prosecutions under its provisions.[16]

---

[15] In 1994, Congress amended the paragraph to emphasize that trespassing upon computers used part-time for the government required a showing that government use was "adversely" affected rather than merely affected, Pub.L.No.103-322, 108 Stat. 2099. Concerned that it might suggest that trespassing could be beneficial, Congress repealed the 1994 amendment in 1996 when it also made changes to make it clear that a person "permitted to access publicly available Government computers . . . may still be convicted under (a)(3) for accessing without authority any nonpublic Federal Government computer" and that a person may be convicted under paragraph (a)(3) for access that affects the use of a computer employed on behalf of the government regardless of whether the computer is actually operated by the government or is merely operated for the government, Pub.L.No. 104-294, 110 Stat. 3491; S.Rep.No. 104-357 at 9 (1996).

[16] Olivenbaum, *<CTRL><ALT><DELETE>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL LAW REVIEW 574, 600-1 (1997); *United States v. Rice*, *aff'g w/o published op.*, 961 F.2d 211 (4th Cir. 1992), subsequent motion for correction of sentence, 815 F.Supp. 158 (W.D.N.C. 1993).

Rice is a curious case. The unpublished opinion indicates that Rice, a long time Internal Revenue Service (IRS) agent, hacked into the IRS computers at the behest of a drug dealer and disclosed to the dealer the status of an IRS investigation of the dealer; the agent also advised the dealer on means of evading forfeiture of his house. For this he was convicted of conspiracy to launder his friend's drug profits (18 U.S.C. 1956(a)(1)(b)(i)), conspiracy to defraud the United States of forfeitable property (26 U.S.C. 7214), computer fraud , i.e., accessing the computer system of a government agency without authority (18 U.S.C. 1030(a)(3)), and unauthorized disclosure of confidential information (18 U.S.C. 1905)(sometimes known as the Trade Secrets Act). The court did not address the apparent conflict between the conviction and the legislative history of paragraph 1030(a)(3) indicating that the paragraph does not govern cases of an employee hacking into the computer systems of his own agency. See also *Brownlee v. Dyncorp*, 349 F.3d 1343 (Fed Cir. 2003) (noting that the defendant to charges under §1030(a)(3) had entered into a plea agreement, and that his employer–a government contractor–was not charged with any criminal actions; the defendant had entered false data regarding hours worked into the government computer system).

Other Crimes.[17]

Attempt.

An attempt to hack into a federal computer in violation of paragraph 1030(a)(3) is also a federal crime, 18 U.S.C. 1030(b). In fact, subsection 1030(b) makes it a federal crime to attempt to violate any of the paragraphs of subsection 1030(a).[18] The subsection dates from the original enactment and evokes no comment in the legislation history other than the notation of its existence, H.R.Rep.No. 98-894 at 22 (1984).

This is not particularly unusual. There is no general federal attempt statute,[19] but Congress has elected to penalize attempts to commit many individual federal crimes.[20] A body of case law has grown around them that provides a common understanding of their general dimensions. Thus, as a general rule, in order to convict a defendant of attempt, the government must prove beyond a reasonable doubt that, acting with the intent required to commit the underlying offense,[21] the defendant took some substantial step towards the commission of the underlying

---

[17] Throughout this report, "other crimes" refers to closely related crimes. In any given case, a defendant charged under one of the paragraphs of 1030(a) may also be charged under one or more of these other federal companion statutes. As long as there is at least one element required for conviction of one but not the other, a defendant guilty of violating one or more of the various paragraphs of section 1030 may also be held liable for one or more related offenses, see e.g. *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997) (convictions under 18 U.S.C. 1343 (wire fraud) and 18 U.S.C. 1030(a)(4) (computer fraud) overturned for other reasons); *United States v. Petersen*, 98 F.3d 502 (9th Cir. 1996) (upholding a sentence imposed for convictions under 18 U.S.C. 371 (conspiracy), 18 U.S.C. 1343 (wire fraud), and 18 U.S.C. 1030(a)(4) (computer fraud)).

Discussion of additional crimes that might have appropriately been included may have been omitted due either to the constraints of time and space or to oversight.

[18] Subsection 1030(b) states in its entirety, "Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section."

[19] *United States v. Neal*, 78 F.3d 901, 906 (4th Cir. 1996); *United States v. Adams*, 305 F. 3d 30, 34 (1st Cir. 2002).

[20] *See e.g.,* 18 U.S.C. 1951 (attempt to obstruct interstate commerce by extortion or robbery); 18 U.S.C. 794 (attempt to communicate national defense information to a foreign government). There are separate attempt offenses in over 130 sections of title 18 alone: e.g., 18 U.S.C. 32, 33, 37, 112, 115, 152.

[21] *United States v. Barnes*, 230 F.3d 311, 314 (7th Cir. 2000); *United States v. Plummer*, 221 F.3d 1298, 1303 (11th Cir. 2000); *United States v. Ballinger*, 395 F.3d 1218, 1238 n.8 (11th Cir. 2005).

offense[22] that strongly corroborates his criminal intent.[23] Mere preparation does not constitute a substantial step.[24] The line between preparation and a substantial step towards final commission depends largely upon the facts of a particular case,[25] and the courts have offered varying descriptions of its location.[26]

Conspiracy.

Conspiracy to violate any federal law is a separate federal crime, 18 U.S.C. 371,[27] Thus, if two or more individuals agree to intentionally access a government computer without authorization and one of them takes some affirmative action to effectuate their plan, each of the individuals is guilty of conspiracy under section 371,

---

[22] *United States v. Smith*, 264 F.3d 1012, 1015 (10th Cir. 2001); *United States v. Herrera*, 289 F.3d 311, 318 (5th Cir. 2002); *Ballinger*, 395 F.3d at 1238 n.8; *United States v. Munro*, 394 F.3d 865, 869 (10th Cir. 2005); *United States v. Bellew*, 369 F.3d 450, 453 n.2 (5th Cir. 2004).

[23] *United States v. Crow*, 164 F.3d 229, 235 (5th Cir. 1999); *United States v. Burns*, 298 F.3d 523, 539 (6th Cir. 2002); *Bellew*, 369 F.3d 450, 453 n.2.

[24] *United States v. Bailey*, 228 F.3d 637, 640 (6th Cir. 2000); *United States v. Yousef*, 327 F.3d 56, 79 (2d Cir. 2003); *Ballinger*, 395 F.3d at 1238 n.8; *United States v. Murrell*, 368 F.3d 1283, 1286 (11th Cir. 2004).

[25] *United States v. Barnes*, 230 F.3d 311, 315 (7th Cir. 2000); *United States v. Plummer*, 221 F.3d 1298, 1303 (11th Cir. 2000); *United States v. Ramirez*, 348 F.3d. 1175, 1180 (10th Cir. 2003).

[26] *United States v. Yossunthorn*, 167 F.3d 1267, 1271 (9th Cir. 1999)("When criminal intent is clear, identifying the point at which the defendants' activities ripen into an attempt is not an analytically satisfying exercise. Nevertheless, the requirements are distinct; even when the defendant's intent is clear, his actions must cross the line between preparation and attempt by unequivocally demonstrating that the crime will taken place unless interrupted by independent circumstances); *United Stats v. LiCausi*, 167 F.3d 36, 47 (1st Cir. 1999)("To prove attempt, the government must establish an intent to commit the substantive offense and a substantial step towards its commission that is less than the last act necessary to commit the crime itself"); *United States v. Ramirez*, 348 F.3d. 1175, 1180 (10th Cir. 2003)(noting that a substantial step "must be an act adapted to, approximating, and which in the ordinary and likely course of things will result in, the commission of the particular crime. A substantial step is an appreciable fragment of a crime and an action of such substantiality that, unless frustrated, the crime would have occurred. The step must be strongly corroborative of the firmness of the defendant's criminal intent and must unequivocally mark the defendant's acts as criminal. It should evidence commitment to the criminal venture")(citing *United States v. Smith*, 264 F.3d 1012, 1016 (10th Cir. 2001)).

[27] "If two or more persons conspire . . . to commit any offense against the United States . . . or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

"If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor," 18 U.S.C. 371; see generally, *Nineteenth Survey of White Collar Crime: Federal Criminal Conspiracy*, 41 AMERICAN CRIMINAL LAW REVIEW 611 (2004); *Developments in the Law – Criminal Conspiracy*, 72 HARVARD LAW REVIEW 920 (1959).

regardless of whether the scheme is ultimately successful;[28] and if a conspirator manages to "hack" into a government computer, his coconspirators are equally guilty under 18 U.S.C. 1030(a)(3).[29]

Accomplices as Principals.

By the same token, one who counsels, commands, aids or abets, or otherwise acts as an accessory before the fact is liable as a principal for the underlying substantive offense to the same extent as the individual who actually commits the offense.[30] More than mere inadvertent assistance is required; but an accomplice who embraces the criminal objectives of another and acts to bring about their accomplishment is criminally liable as a principal.[31]

---

[28] *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000) ("conspirators need not succeed in completing the underlying [crime], nor need that underlying act even be factually possible"); *United States v. Bond*, 231 F.3d 1075, 1079 (7th Cir. 2000) ("[a]s with any conspiracy allegation, the government need not prove a completed underlying crime"); *United States v. Nelson-Rodriguez*, 319 F.3d 12, 28 (1st Cir. 2003) ("A conspiracy need not succeed for a conspiracy conviction to stand. Indeed, the underlying act need not even be attempted"); *United States v. Tucker*, 376 F.3d 236, 238 (4th Cir. 2004) ("Proof of a conspiracy does not require proof that the object of the conspiracy was achieved or could have been achieved, only that the parties agreed to achieve it.").

[29] *Pinkerton v. United States*, 328 U.S. 640, 645-48 (1946); *United States v. Long*, 301 F.3d 1095, 1103 (9th Cir. 2002)("The *Pinkerton* doctrine is a judicially-created rule that makes a conspirator criminally liable for the substantive offenses committed by a co-conspirator when they are reasonably foreseeable and committed in furtherance of the conspiracy"); *United States v. Carrington*, 301 F.3d 204, 211 (4th Cir. 2002). *United States v. Hayes*, 391 F.3d 958, 962 (8th Cir. 2004) ("each member of a conspiracy may be held criminally liable for any substantive crime committed by a co-conspirator in the course and furtherance of the conspiracy, even though those members did not participate in or agree to the specific criminal act."); *United States v. Silvestri*,__F.3d__, No. 03-12820, 2005 WL 1208510, at *21 (11th Cir. May 23, 2005) ("conspirators are liable for all of the acts and foreseeable consequences of the conspiracy").

[30] "(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

"(b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal," 18 U.S.C. 2; see generally, Blakey & Roddy, *Reflections on* Reves v. Ernst & Young*: Meaning and Impact on Substantive, Accessory, Aiding Abetting and Conspiracy Liability Under RICO*, 33 AMERICAN CRIMINAL LAW REVIEW 1345, 1385-418 (1996); see also*, United States v. Yakou*, 393 F.3d 231, 242 (D.C. Cir. 2005)("The statute typically applies to any criminal statute unless Congress specifically carves out an exception that precludes aiding and abetting liability, and it long has been established that a person can be convicted of aiding and abetting another person's violation of a statute even if it would be impossible to convict the aider and abettor as a principal")(citations omitted).

[31] *United States v. Ramirez-Velasquez*, 322 F.3d 868, 880 (5th Cir. 2003)("to establish aiding and abetting under 18 U.S.C. 2, the government must show that the defendant (1) associated with a criminal venture, (2) participated in the venture, and (3) sought by action to make the venture successful"); *United States v. Garcia*, 400 F.3d 816, 819n.2 (9th Cir. 2005) ("For aiding and abetting liability the government must prove four elements: (1) that the accused had the specific intent to facilitate the commission of a crime by another, (2)

The fact that subsection 1030(b) outlaws attempts to violate any of the prohibitions of subsection 1030(a) raises an interesting question concerning accessories. As a general rule, an accomplice may only be liable as a principal or accessory before the fact, for a completed crime; the aid must be given before the crime is committed, but liability as a principal will not attach until after the crime has been committed.[32] This does not bar conviction of one who aids or abets the commission of a crime that never succeeds beyond the attempt phase, if, as in the case of paragraph 1030(a)(3), attempt to commit the offense has been made a separate crime.[33]

CAN-SPAM, Paragraph 1030(a)(2), & e-mail.

Beyond these auxiliary offenses and bases for criminal liability, the simple trespassing crime created in paragraph 1030(a)(3) is the least likely of the seven crimes established in section 1030 to overlap with other laws. Simply hacking into government computers – without damage to the system, injury to the government, or gain by the hacker – implicates only a few other laws.

The most likely overlap would be with the CAN-SPAM Act of 2003, 18 U.S.C. 1037. The CAN-SPAM Act offers protection to all "protected computers"[34] and prohibits any unauthorized access of these computers when for the purpose of sending commercial electronic messages (1037(a)(1)), as well as even authorized use if the use involves deceiving or misleading e-mail recipients (1037(a)(2)). The penalties involved for a violation of CAN-SPAM can be as high as 5 years

---

that the accused had the requisite intent of the underlying substantive offense, (3) that the accused assisted or participated in the commission of the underlying substantive offense, and (4) that someone committed the underlying substantive offense."); *United States v. Davis*, 306 F.3d 398, 412 (6th Cir. 2002)("the essential elements of aiding and abetting are (1) an act by the defendant that contributes to the commission of the crime and (2) an intention to aid in the commission of the crime"); *United States v. Harris*, 397 F.3d 404, 415 (6th Cir. 2005)(same).

[32] *United States v. Richards*, 302 F.3d 58, 67 (2d Cir. 2002)("To sustain a verdict on an aiding and abetting theory, the evidence must show that the underlying crime was committed by someone other than the defendant and that the defendant himself either acted or failed to act with the specific intent of advancing the commission of the underlying crime"); *United States v. Cartwright*, 359 F.3d 281, 287 (3d Cir. 2004) (an aiding and abetting conviction "requires that another committed the substantive offense and that the one charged with aiding and abetting knew of the substantive-offense commission and acted with the intent to facilitate it.") *United States v. Keene*, 341 F.3d 78, 84 (1st Cir. 2003)("a defendant may be convicted as an aider and abettor if the evidence shows: (1) that the underlying offense was committed by a principal. . .").

[33] *United States v. Washington*, 106 F.3d 983, 1004-5 (D.C.Cir. 1997)("if the principal had actually attempted to commit a crime but had failed, the aider and abettor would be charged with the same offense as the principal (attempt to commit the crime)"). See also *United States v. Villanueva*, 408 F.3d 193, 202 (5th Cir. 2005) (finding defendant guilty of aiding and abetting an attempted crime).

[34] The definition of "protected computer" in section 1037 defers to the definition in 1030(e)(2(B), which covers any computer "used in interstate or foreign commerce or communication" and implicates any computer connected to the internet.

imprisonment if done in furtherance of a felony, or 3 years for a violation of (a)(1) or if there is any financial loss by the victim or gain by the hacker, or 1 year "in any other case", 18 U.S.C. 1037(b)[35]. Trespassing may also breach the "hacking-and-acquiring-information" ban of paragraph 1030(a)(2), discussed *infra*. It may also violate one of the state computer crime statutes.[36] Hacking into someone else's e-mail stored in a government computer system seems contrary to both paragraph 1030(a)(3) and to the federal statute that protects e-mail and stored telephone company records, 18 U.S.C. 2701.[37]

---

[35] CAN-SPAM is discussed more in depth *infra* in relation to section 1030(a)(4) on Computer Fraud.

[36] Most states have statutes which on their faces appear to outlaw simple computer trespassing: ALA.CODE §13A-8-102; ALASKA STAT. §11.46.484; ARIZ.REV.STAT.ANN. §13-2316.02; ARK.CODE ANN. §5-41-104; CAL. PENAL CODE §502; COLO.REV.STAT.ANN. §18-5.5-102; CONN.GEN.STAT.ANN. §53a-251; DEL.CODE ANN. tit.11 §932; FLA.STAT.ANN. §815.06; HAWAII REV.STAT. §708-892, 892.5; IDAHO CODE §18-2202; ILL.COMP.STAT. ANN. 720 5/16D-3; IND.CODE ANN. §35-43-2-3; IOWA CODE ANN. §716.6B, 702.1A; KAN. STAT.ANN. §21-3755(d); KY.REV.STAT.ANN. §434.845, 850; LA.REV.STAT.ANN. §14:73.2; ME. REV.STAT.ANN. tit.17-A §432; MD.CRIM.CODE ANN. §7-302; MASS.GEN.LAWS ANN. ch.266 §120F; MINN.STAT.ANN. §609.891; MISS.CODE ANN. §97-45-9; MO.ANN.STAT. §569.099; MONT.CODE ANN. §45-6-311; NEB.REV.STAT. §28-1347; NEV.REV.STAT. §205.4765; N.H. REV.STAT.ANN. §638:17; N.J. STAT.ANN. §2A:38A-3, §2C:20-25; N.Y. PENAL LAW §156.10; N.C.GEN. STAT. §14-454; N.D.CENT. CODE §12.1-06.1-08; OHIO REV. CODE ANN. §2913.04(B); OKLA. STAT.ANN. tit.21 §1953; ORE.REV.STAT. §164.377; PA.STAT.ANN. tit.18 §§7611, 7615; R.I.GEN. LAWS §11-52-3; S.C.CODE ANN. §16-16-20(4); S.D.COD.LAWS §43-43B-1; TENN.CODE ANN. §39-14-602; TEX.PENAL CODE ANN. §33.02; UTAH CODE ANN. §76-6-703; VT.STAT. ANN. tit.13 §4102; WASH. REV.CODE ANN. §9A.52.110, 120; W.VA.CODE ANN. §61-3C-5; WIS. STAT.ANN. §943.70; WYO. STAT. §6-3-504. At least one state permits dismissal of computer abuse charges based upon the absence of damage, HAW.REV.STAT. §708-892, and a few only outlaw hacking in the presence of an addition element such as damage or an intent to defraud, GA.CODE ANN. §16-9-93; MICH.COMP.STAT. ANN. §§752.791 to 797; N.MEX.STAT.ANN. §§30-45-1 to 30-45-7; VA.CODE §§18.2-152.1 to 18.2-152.15. Analysis of state law is generally beyond the scope of this report.

Members of the military may also incur liability under the Uniform Code of Military Justice for various forms of computer abuse. See *United States v. Wiest*, 59 M.J. 276 (Ct. App. Armed Forces 2004) (reversing lower court on other grounds) in which an Air Force Academy cadet was convicted of a violation of Article 134 of the Uniform Code of Military Justice, for accessing a protected computer without authorization and recklessly damaging a computer in violation of 18 U.S.C. § 1030(A)(5)(B)). See also, *United States v. Mervine*, 26 M.J. 482 (1988)(suggesting that various computer crimes might be charged under Article 134, the general article: "Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special, or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court");

[37] "(a) Offense.– Except as provided in subsection (c) of this section whoever – (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided

Hackers who misidentify themselves in order to gain access to a federal computer may be guilty of violating 18 U.S.C. 1001[38] and 18 U.S.C. 912[39] in the view of at least one commentator.[40] The case law may make the claim difficult to

---

in subsection (b) of this section.

"(b) Punishment.– The punishment for an offense under subsection (a) of this section is– (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State– (A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and (B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and (2) in any other case– (A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

"(c) Exceptions.–Subsection (a) of this section does not apply with respect to conduct authorized– (1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user; or (3) in section 2703, 2704 or 2518 of this title," 18 U.S.C. 2701.

The provisions of 18 U.S.C. 2511 (wiretapping) may apply to the unlawful interception of e-mail transmissions while in transit and 18 U.S.C. 2701 may apply to the unlawful seizure of stored e-mail.

[38] "(a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully – (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined under this title or imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both.

"(b) Subsection (a) does not apply to a party to a judicial proceeding, or that party's counsel, for statements, representations, writings or documents submitted by such party or counsel to a judge or magistrate in that proceeding.

"(c) With respect to any matter within the jurisdiction of the legislative branch, subsection (a) shall apply only to – (1) administrative matters, including a claim for payment, a matter related to the procurement of property or services, personnel or employment practices, or support services, or a document required by law, rule, or regulation to be submitted to the Congress or any office or officer within the legislative branch; or (2) any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission or office of the Congress, consistent with applicable rules of the House or Senate," 18 U.S.C. 1001; see generally, *Nineteenth Survey of White Collar Crime: False Statements*, 41 AMERICAN CRIMINAL LAW REVIEW 545 (2004).

[39] "Whoever falsely assumes or pretends to be an officer or employee acting under the authority of the United States or any department, agency or officer thereof, and acts as such, or in such pretended character demands or obtains any money, paper, document, or thing of value, shall be fined under this title or imprisoned not more than three years, or both," 18 U.S.C. 912.

[40] Olivenbaum, *<CTRL><ALT><DELETE>: Rethinking Federal Computer Legislation*, 27 SETON HALL LAW REVIEW 574, 600 (1997)(citing an instance from the infancy of section 1030 where a hacker was indicted under the false statement, 18 U.S.C. 1001, and wire fraud, 18 U.S.C. 1343, statute. The case ended when the defendant pled to a misdemeanor fraud

defend. The Supreme Court has suggested that section 1001 should be constructed narrowly,[41] and the courts have consistently held that the false statement must somehow tend to adversely impact the functioning of a governmental agency or department to trigger coverage under section 1001.[42] Cases in other contexts demonstrate the difficulty of convincing the courts that simple trespassing in government cyberspace has an adverse impact upon the government.[43]

The difficulty with using the impersonation statute, 18 U.S.C. 912, is that it requires a showing of an official act or of a fraud; something that need not be proven for conviction under paragraph 1030(a)(3).[44] Like 18 U.S.C. 1001, section 912 may be more appropriately employed in cases falling under the ambit of paragraph 1030(a)(4) (unauthorized access of a government computer, bank computer or computer in interstate or foreign commerce as integral part of a scheme to fraud).

Obtaining Information by Unauthorized Computer Access 18 U.S.C. 1030(a)(2)

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

---

charge). No comparable prosecutions followed and so the author's thesis remains unproven.

[41] *Hubbard v. United States*, 514 U.S. 695 (1995)(overturning a longstanding holding that section 1001 applied to false statements made to federal courts and to Congress as well as those made to the executive branch)(superceded by statute, Pub.L. 104-292, 110 Stat. 3459 (1996)(the modification preserved the exception that it did not apply "to a party to a judicial proceeding, or that party's counsel, for statements, representations, writings or documents submitted by such party or counsel to a judge or magistrate in that proceeding.")(section 1001(b)).; *United States v. Gaudin*, 515 U.S. 509 (1995)(holding that materiality of the false statement, as an element of section 1001, is a question for the jury to decide).

[42] *United States v. Gaudin*, 515 U.S. 506, 509 (1995)("the statement must have a natural tendency to influence, or be capable of influencing the decision of the decisonmaking body to which it was addressed"); *United States v. Baker*, 200 F.3d 558, 561 (8th Cir. 2000) ("The materiality inquiry focuses on whether the false statement had a natural tendency to influence or was capable of influencing the government agency or official"). *United States v. Mitchell*, 388 F.3d 1139, 1143 (8th Cir. 2004) (noting that a false statement must have "a natural tendency to influence or is capable of influencing the government agency or official" and that "[m]ateriality does not require proof that the government actually relied on the statement.").

[43] *United States v. Collins*, 56 F.3d 1416 (D.C.Cir. 1995) and *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), overturned convictions under 18 U.S.C. 641 (theft of government property), and 18 U.S.C. 1343 (wire fraud) and 1030(a)(4)(computer fraud) respectively, on the ground that the prosecution had failed to show any adverse impact upon the government caused by the defendant's unauthorized access of government computer files.

[44] "Whoever . . . pretends to be an officer . . . acting under the authority of the United States . . . *and acts as such, or in such pretended character demands or obtains any . . . thing of value*," 18 U.S.C. 912 (emphasis added).

(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,[45] *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.);*[46]

(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.

One step beyond simple hacking is the prohibition against acquiring certain protected information by intentional unauthorized access.[47] As a practical matter, in

---

[45] "The term 'card issuer' means any person who issues a credit card, or the agent of such person with respect to such card," 15 U.S.C. 1602(n).

"The term 'person' means a natural person or an organization. The term 'organization' means a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association. The term 'credit card' means any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit. The term 'credit' means the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment.

"The term 'creditor' refers only to a person who both (1) regularly extends, whether in connection with loans, sales of property or services, or otherwise, consumer credit which is payable by agreement in more than four installments or for which the payment of a finance charge is or may be required, and (2) is the person to whom the debt arising from the consumer credit transaction is initially payable on the face of the evidence of indebtedness or, if there is no such evidence of indebtedness, by agreement. Notwithstanding the preceding sentence, in the case of an open-end credit plan involving a credit card, the card issuer and any person who honors the credit card and offers a discount which is a finance charge are creditors . . ." 15 U.S.C. 1602(d), (c),(k), (e), and (f), respectively.

[46] "The term 'file', when used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

"The term 'consumer reporting agency' means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

"The term 'consumer' means an individual," 15 U.S.C. 1681a(g), (f) and (c), respectively.

[47] "Without authorization" or "exceeds authorized access" under 1030(a)(2) has been determined by courts to apply to current authorized employees when doing so for unauthorized purposes, and former employees as well. *Shurgard Storage Centers v. Safeguard Self Storage*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (unauthorized access found when employees used their access to benefit a competitor); *YourNetDating v. Mitchell*, 88 F. Supp. 2d 870 (N.D. Ill. 2000) (former employee found to be exceeding authorized access because he used his access codes to divert users from his ex-employers website). Furthermore, "access" within this statute does not mean simply using a computer

any instance involving a government computer it may be very difficult to distinguish between cases evidencing a violation of the simple trespass proscriptions of paragraph 1030(a)(3) and the trespassing-with-information-acquisition prohibitions of paragraph 1030(a)(2).

Jurisdiction.

Paragraph 1030(a)(2), unlike 1030(a)(3), covers more than government computers. It covers three types of information – information of the federal government, consumer credit or other kinds of financial information, and information acquired through interstate or foreign access.

The protection for financial information has its origins in the initial legislation and was among the first adjusted. Comments from the Senate report accompanying the 1986 amendments illustrate the intended scope of the protection for financial information:

> "The 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. This protection is imperative in light of the sensitive and personal financial information contained in such computer files. However, by referring to the Right to Financial Privacy Act, the current statute limits its coverage to financial institution customers who are individuals, or are partnerships with five or fewer partners. The Committee intends . . . to extend the same privacy protections to the financial records of all customers – individual, partnership, or corporate – of financial institutions.
>
> "The Department of Justice has expressed concerns that the term 'obtains information' in 18 U.S.C. 1030(a)(2) makes that subsection more than an unauthorized access offense, i.e., that it might require the prosecution to prove asportation of the data in question. 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. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection," S.Rep.No. 99-432 at 6-7 (1986).

The committee explanation of the language amending paragraph 1030(a)(2), ultimately enacted as part of the Economic Espionage Act of 1996, endorsed this reading and extended it to cover information obtained from federal computers and information secured by interstate cyberspace trespassing:

> "'Information' as used in this subsection [1030(a)(2)] includes information stored in intangible form. Moreover, the term 'obtaining information' includes

---

or passively receiving information from a computer. *Role Models America v. Jones*, 305 F. Supp. 2d 564, 566-7 (D.Md.2004) (court rejected claim that a university "accessed" a computer when a high school employee sent them information from a school computer). For additional analysis on the meanings of these terms, see generally, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" & "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L.R. 1596 (2003).

> merely reading it. 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. This interpretation of 'obtaining information' is consistent with congressional intent expressed . . . in connection with 1986 amendments to the Computer Fraud and Abuse statute . . . .
>
> "The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer. This information, stored electronically, is intangible, and it has been held that the theft of such information cannot be charged under more traditional criminal statutes such as Interstate Transportation of Stolen Property Act, 18 U.S.C. 2314. See *United States v. Brown*, 925 F.2d 1301, 1308 (10th Cir. 1991). This subsection 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. In instances where the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws. The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information," S.Rep.No. 104-357 at 6-7 (1996).

The precise relationship of this paragraph, 1030(a)(2), to the simple trespass provisions of paragraph 1030(a)(3) in cases of government computer stored information is somewhat unclear. The history of the trespass provisions speaks clearly of an intent to place beyond their reach whistleblowers and other federal employees for simple trespassing with respect to computers within their own an agency. This explains the absence of an "exceeds-authorized-access" provision in the trespassing provisions of paragraph 1030(a)(3). But the trespass-and-be-exposed-to-information provisions of paragraph 1030(a)(2) *do* feature a "exceeds-authorized-access" clause and seem facially applicable to whistleblowers. It remains to be seen whether the courts will read paragraph 1030(a)(2) as effectively amending the simple trespassing provisions of paragraph 1030(a)(3) or will attempt to reconcile the two.

Intent.

The intent requirement is the same as that required in the case of simple trespassing. The offender must have "intentionally" gained access. The paragraph only bans "intentional" trespassing. As in the case of the simple trespassing the intent element can be satisfied by anyone who purposefully gains access to a computer covered by the paragraph or by anyone "whose initial access was inadvertent but who then deliberatively maintain access after a non-intentional initial contact," H.R.Rep.No. 99-612 at 9-10 (1986); see also, S.Rep.No. 99-432 at 5-6 (1986).

Penalties.

Paragraph 1030(a)(2) has a three tier sentencing structure. Simple violations are punished as misdemeanors, imprisonment for not more than 1 year and/or a fine of not more than $100,000 ($200,000 for organizations), 18 U.S.C. 1030(c)(2)(A).

The second tier carries penalties of imprisonment for not more than 5 years and/or a fine of not more $250,000 ($500,000 for organizations) and is reserved for

cases in which: "(i) the offense was committed for purposes of commercial advantage or private financial gain; (ii) the offense was 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 (iii) the value of the information obtained exceeds $5,000," 18 U.S.C. 1030(c)(2) (B).

This second level was added in 1996. The $5,000 threshold is the same one the section uses to separate serious from less serious fraud and destruction cases in paragraphs 1030(a)(4) and 1030(a)(5). With respect to the alternative thresholds, (i) and (ii), "[t]he 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 the wiretap statute (18 U.S.C. 2511[(2)] (d)), respectively, and are intended to have the same meaning as in those statutes," S.Rep.No. 104-357 at 8 (1996). The references to copyright and wiretap law may be less instructive than Congress anticipated for the phrases in question are of uncertain meaning in their original settings.[48] Nevertheless, they clearly contemplate some criminal, tortious, or financially advantageous purpose beyond the computer-trespassing-and-obtaining-information misconduct outlawed in the paragraph generally. Otherwise nothing would be left to be punished as a misdemeanor and the $5,000 distinction of exception (iii) would be swallowed up as well.

The third tier is for repeat offenders whose punishment is increased to imprisonment of not than 10 years and/or a fine of not more than $250,000 ($500,000 or organizations) for a second or subsequent conviction, 18 U.S.C. 1030(c).

The theft, embezzlement, and fraud Sentencing Guideline applies to violations of paragraph 1030(a)(2), U.S.S.G. §2B1.1 (base offense level 6). It has the same 2 level increase as applies to violations of paragraph 1030(a)(3)(simple hacking) when the victimized computer is used as for critical infrastructure or is used by a government entity for national security, defense, or criminal justice purposes. It carries a 6 level increase (and a minimum offense level of 24), however, when the offenses causes a substantial disruption of a critical infrastructure. Moreover, when the violation results in a loss of more than $5,000, addition offense levels ranging from 2 to 30 may be assessed depend upon the extent of the loss; and when the violation victimizes 10 or more individuals or entities, additional offenses ranging from 2 to 6 may be tacked on.

---

[48] 4 NIMMER & NIMMER, NIMMER ON COPYRIGHT §15.01 n.1.2 (1997) (emphasis added)("*Apparently*, the phrase 'commercial advantage or private financial gain' is intended as the equivalent of 'for profit'"); 1 FISHMAN & MCKENNA, WIRETAPPING AND EAVESDROPPING, SECOND EDITION §4:29 *b.* (1995) comparing, *Stockler v. Garratt*, 893 F.2d 856 (6th Cir. 1990), with, *By-Product Corp. v. Armen-Berry Co.*, 668 F.2d 956 (7th Cir. 1982)(in disagreement over whether an offender must act upon his or her criminal or tortious purpose after recording a conversation to which they are a party or where one party to the conversation has consented to the recording).

Regardless of the criminal sanctions imposed, offenders of paragraph 1030(a)(2) may also incur civil liability for damage caused, 18 U.S.C. 1030(g).[49]

Other Crimes.

Attempt, Conspiracy, and Complicity.

The same general observations concerning attempt, conspiracy and aiding and abetting noted for the simple trespass offense apply here. It is a separate crime to attempt to violate paragraph 1030(a)(2) under 18 U.S.C. 1030(b). Those who attempt to violate its provisions or aid and abet the violation of another are subject to the same penalties as those who commit the substantive offense, 18 U.S.C. 1030(c)(2). The same is true of conspirators unless the underlying offense is a felony in which case the maximum penalty is imprisonment for not more than 5 years and/or a fine of not more than $250,000, 18 U.S.C. 371.

Paragraph 1030(a)(2) is somewhat unique. There are a host of other federal conversion statutes, but all of the others appear to require that the offender either commit embezzlement by failing to comply with some fiduciary obligation or commit larceny by intending to acquire the property or to deprive another of it. Paragraph 1030(a)(2) in contrast to the conversion statutes and to the computer fraud provisions of paragraph 1030(a)(4) requires no larcenous intent. As a practical matter, it essentially gives prosecutors a more serious charge against hackers who do more than simply breach the outskirts of a governmental system than would be available under the pure trespassing provisions of paragraph 1030(a)(3). And it gives

---

[49] "(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware," 18 U.S.C. 1030(g).

The damages described in clauses (a)(5)(B)(i) through (v) are: "(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security." See, *America Online, Inc. v. National Health Care Discount, Inc.,* 174 F.Supp.2d 890, 899 (N.D. Iowa 2001)(sending bulk unauthorized and unsolicited e-mail to the Internet service provider's customers violated paragraph 1030(a)(2)).

Although subsection 1030(g) applies to any violation under any of the paragraphs of section 1030, it is discussed at greater length below in connection with paragraph 1030(a)(5)(relating to inflicting damage upon a computer).

them an alternative or additional charge, along with conversion and fraud statutes, against hackers who "steal" information from a protected computer.[50]

Paragraph 1030(a)(2) is essentially paragraph 1030(a)(3) plus an information acquisition element and with a broader jurisdictional base. Criminal prohibitions like those of 18 U.S.C. 1001 (false statements on a matter with the jurisdiction of a federal agency) or 912 (impersonating a federal official) which overlap with paragraph 1030(a)(3) at the point of unauthorized entry will overlap with paragraph 1030(a)(2) at the same point. If unauthorized access in violation of paragraph 1030(a)(3) is acquired by false statement under facts sufficient supporting a prosecution under 18 U.S.C. 1001 (false statements) or 18 U.S.C. 912 (false impersonation), unauthorized access and the acquisition of information in violation of paragraph 1030(a)(2) acquired by false statement or impersonation is likely to be subject offender to prosecution under sections 1001 or 912 as well. By the same token, if unauthorized computer access to a voice mail or e-mail communication that violates paragraph 1030(a)(3) offends 18 U.S.C. 2511 (interception of wire or electronic communications) and 2701 (unauthorized acquisition of communications in electronic storage), unauthorized computer access and acquisition of information in violation of paragraph 1030(a)(2) is to violate sections 2511 and 2701.[51]

In fact, overlap is even more likely. Paragraph 1030(a)(3) protects only federal computers. Paragraph 1030(a)(2) protects not only federal computer information, but information from "protected computers" (computers used in interstate and foreign commerce) when the unauthorized access involves an interstate or foreign communication. Due to the nature of the electronic communications, a communication may involve interstate communications even if the both the parties are located within the same state;[52] and, by virtue of an amendment in the USA PATRIOT Act, protected computer information may include information on computers located overseas as long as they involve or affect the foreign commerce or communications of the United States.[53]

---

[50] See, *United States v. Jordan*, 316 F.3d 1215, 1223-224 (11th Cir. 2003)(noting the indictment of a sheriff, for improper use of access to the FBI's NCIC database, under paragraph 1030(a)(2), 18 U.S.C. 2 (aiding and abetting), 371 (conspiracy), and 641 (theft of federal property); the overlap between section 1030 and federal laws that prohibit the theft of intangible property under various circumstances is discussed at greater length in the examination of paragraph 1030(a)(4)(fraud), *infra*.

[51] See, *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875-80 (9th Cir. 2002)(discussing the application of 18 U.S.C. 2511 and 2701 to a case of unauthorized access to a secure website). See also *Motorola Credit Corp. v. Uzan*, 388 F.3d 39, 44 (2d Cir. 2004) (discussing civil suit claiming violations of sections 1030, 2511, and 2701).

[52] *United States v. Kammersell*, 196 F.3d 1137, 1138-140 (10th Cir. 1999)(a threat communicated between two computers in Utah involved interstate communications because the communication was forwarded by way of AOL's server in Virginia).

[53] "[T]he term 'protected computer' means a computer – (A) 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 (B) which is used in interstate or foreign commerce or

Causing Computer Damage
18 U.S.C. 1030(a)(5)

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[54] *without authorization, to a protected computer;*[55]

(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 subparagraph (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 medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security . . . shall be punished as provided in subsection (c) of this section.

---

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)(language added in the USA PATRIOT Act in italics).

[54] "The term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information. . . the term 'loss' means an 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," 18 U.S.C. 1030(e)(8), (11).

[55] "As used in this section . . . (2) the term 'protected computer' means a computer - (A) 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 (B) which is 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).

Intent.

Hackers or the creators of viruses, worms or the like, who damage the systems they invade, even unintentionally, may trigger paragraph 1030(a)(5).[56] Paragraph 1030(a)(5) establishes three computer damage offenses, distinguishable on the basis of the offender's intent: (1) *causing damage* to a protected computer by intentional unauthorized access; (2) *recklessly causing damage* to a protected computer by intentional unauthorized access; and (3) *intentionally causing damage* to a protected computer through a knowing transmission. This feature, added in 1996 and amended in the USA PATRIOT and Homeland Security Acts, punishes recklessly and intentionally caused damage more seriously but preserves the earlier understanding that anyone who intentionally secures unauthorized access is punishable regardless of whether they intended to cause damage, or were recklessly indifferent as to whether they did so.[57]

Damage.

The paragraph covers only five specific kinds of damage inflicted upon a specific class of computers. The damage must be an "impairment to the integrity or availability of data, a program, a system, or information," 18 U.S.C. 1030(e)(8), that:

- causes a loss over the course a year exceeds $5,000 (or for purposes of federal prosecution or suit, damage to more than one "protected computer");
- modifies, impairs, or could modify or impair medical services;
- causes physical injury;

---

[56] *United States v. Lloyd*, 269 F.3d 228, 231 (3d Cir. 2001) involved a former employee charged with triggering a "time bomb" which purged the design and production computer files of the company that fired him. See also, *United States v. Mitra*, 405 F.3d 492 (7th Cir. 2005)(where defendant was found guilty of violating 1030(a)(5) after he disrupted police department's computer-based radio system and thus created public safety problems because the officers could no longer communicate with each other).

[57] Even under an earlier version of the paragraph 1030(a)(5) that outlawed "intentional access . . . without authorization, and by means of . . . such conduct . . . prevent[ing] authorized use of any such computer . . . and thereby causes loss to one or more others of a value aggregating $1,000 or more . . . ," the government was not required to show that the defendant intentionally prevented use nor that he intentionally caused damage "aggregating $1,000 or more"; a demonstration that he intentionally accessed a protected computer without authorization was sufficient, *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991)(Morris, a computer graduate student, was convicted under 18 U.S.C. 1030(a)(5) for releasing a "worm" on the Internet that "spread and multiplied, eventually causing computers at various educational institution and military sites to crash or cease functioning," 928 F.2d at 505); *United States v. Sablan*, 92 F.3d 865, 868 (9th Cir. 1996). Sablan, a disgruntled former bank employee, surreptitiously entered the bank after hours and "called up" and damaged several files from the bank's mainframe on the computer to which she had been assigned prior to her discharge.

- threatens public health or safety; or

- affects a justice, national defense, or national security entity computer, 18 U.S.C. 1030(a)(5)(B).

This last element (affects various government computers) and the elimination of the $5,000 threshold requirement for protected computers in the first element emerged as part of the USA PATRIOT Act realignment, adjustments accomplished without a great deal of specific explanation.[58]

The other elements were added in 1996 without a great deal of individual commentary,[59] but the 1996 legislative history of related segments of the statute is informative. An earlier prohibition spoke of intrusions that "cause[d] *loss or damage* to one or more other persons of value aggregating $1,000 or more during any 1-year period," 18 U.S.C. 1030(a)(5)(A)(ii)(II)(1994 ed.)(emphasis added). The Senate Committee report observes that use of the term "damage" contemplates the inclusion of all economic harm attributable to the intrusion and that the increased dollar limitation is expected to restrict federal felony prosecutions to the more serious cases:

> "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 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 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 resecuring 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. As in the past, the term 'damage' will require . . . significant financial losses," S.Rep.No. 104-357 at 11 (1996).

Ordinarily, the presence of a separate hacker prohibition with less severe penalties would argue against allowing "damage assessment" and "security enhancement" costs to be used to reach the $5,000 threshold for the more severe penalty. The report language might be read to rebut such a presumption, but it might

---

[58] The USA PATRIOT Act changes were not among those initially requested by the Administration, *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary,*107th Cong., 1st Sess. (2001). Nor do they appear in the House Committee reports of the bills which ultimately became part of the Act, H.R.Rep.No. 107-236 (2001); H.R.Rep.No. 107-250. There were no Senate committee reports and the only apparent reference to them in the debates is terse, 147 *Cong.Rec.* H7200 (daily ed. Oct. 23, 2001). Much of the language had been part a proposal reported out of the Senate Judiciary Committee in the 106th Congress but without a written report, S.2448 (106th Cong.).

[59] See S.Rep.No. 104-357 at 13-4 (1996) (simply paraphrasing the language of the definition).

also be characterized as asserting no more than that the cost of new locks ("resecuring the system") can be considered damage when the keys ("passwords") are stolen.

The USA PATRIOT Act eliminates the prospect of misconception by supplying an explicit definition of "loss" as used here; "the term 'loss' means 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," 18 U.S.C. 1030(e)(11).

The Act also eliminates a second potential problem. The 1996 amendments, perhaps inadvertently, rephrased the aggregate $5,000 damage-loss threshold describing the victims as "individuals" rather than the term previously employed, "persons."[60] The change stimulated contentions that Congress intended to limit the cases where the threshold could be reached entirely to the damages and losses suffered by human beings without any reference to the damages and losses suffered by corporate or other legal entities.[61] The USA PATRIOT Act negates the problem by describing the damage-loss victims as "persons" and by defining persons to include individuals and any "legal or other entity," 18 U.S.C. 1030(a)(5)(B)(ii), (e)(12).

The long standing medical tampering element has no monetary threshold and has remained essentially unchanged since it was added in response to an incident in which juvenile hackers broke into the computer system of the Sloan-Kettering Cancer Center.[62]

The inclusion of computer tampering that causes physical injuries or threatens public health or safety, on the other hand, is new with the 1996 amendments and is designed to reach more general threats:

> "As the NII [National Information Infrastructure] and other network infrastructures continue to grown, computers will increasingly be used for access to critical services such a emergency response systems and air traffic control, and will be critical to other systems which we cannot yet anticipate," S.Rep.No. 104-357 at 11 (1996).

---

[60] Compare, "causes loss or damage to one or more other *persons* of value aggregating $1,000 or more during any 1-year period," 18 U.S.C. 1030(a)(5)(A)(ii)(II)(aa)(1994 ed.) (emphasis added), with, "causes loss aggregating at least $5,000 in value during any 1-year period to one of more *individuals*, 18 U.S.C. 1030(e)(8)(A)(2000 ed.)(emphasis added).

[61] The argument was made but rejected in *United States v. Middleton*, 231 F.3d 1207, 1210 (9th Cir. 2000).

[62] S.Rep.No. 99-432 at 2-3 (1986). The medical records offense had always been tied to the use of interstate computers; 1996 amendments also permit prosecution when the medical records tampering involves one of the other four jurisdictional moorings (i.e., the involvement of federal computers or the computers of financial institutes, or adversely affecting the use of computers by the government or financial institutions).

Jurisdiction.

These kinds of damage are only federal crimes under paragraph 1030(a)(5) if they involve a *protected computer*. There are five types of protected computers or computer systems. The five include computers:

- used exclusively for or by the United States Government;
- used exclusively for or by a bank or other financial institution;
- used in part for or by the United States Government where the damage "affects" the government use or use of the government's behalf;
- used in part for or by a bank or other financial institution where the damage "affects" use by or on behalf of the institution; and
- used in interstate or foreign commerce or communications including a computer outside the country whose use affects U.S. commerce, 18 U.S.C. 1030(e)(2).

What is a "computer . . . used in interstate or foreign commerce or communications"? The legislative history shows that the phrase means computer damage which might affect interstate or foreign commerce or interstate or foreign communications. The phrase appears in section 1030 after the 1994 amendments when it was first used to supplement (and in the 1996 amendments to replace) the phrase "computer . . . which is one of two or more computers used in committing the offense, not all of which are located in the same State," compare 18 U.S.C. 1030(a)(5), (e)(2)(1986 Supp.), with 18 U.S.C. 1030(a)(5), (e)(2)(1994 ed.). The change was made because under the earlier language "hackers who attacked other computers in their own State were not subject to Federal jurisdiction, notwithstanding the fact that their actions may have severely affected interstate or foreign commerce. For example, individuals who attack[ed] telephone switches m[ight] disrupt interstate and foreign calls. The 1994 change remedied that defect," S.Rep.No. 104-357 at 10 (1996).

Precisely which government computers are protected is a bit more uncertain. Although terms used elsewhere in section 1030 such as "governmental entity"[63] and "department of the United States," are expressly defined, there is no definition of either the phrase "United States Government" or the phrase "Government of the United States" used from the beginning to described the scope of protection provided federal computers. The reports do not explain its meaning. In the trespassing provisions of paragraph 1030(a)(3), however, the phrase is used in juxtaposition with

---

[63] "As used in this section . . . (9) the term 'government entity' includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country," 18 U.S.C. 1030(e)(9).

the phrase "department or agency of the United States"[64] suggesting that the term embodies the meaning assigned to that phrase by the definitions subsection of section 1030[65] and by the definition section generally applicable to title 18 of the United States Code.[66] On the other hand, it would not be unreasonable for a court to conclude that the phases "United States Government" and "Government of the United States" should be construed narrowly since when Congress intended an expansive definition it provided one. The definition of financial institutions whose computers are protected[67] differs only slightly from the definition generally applicable in title 18.[68]

---

[64] "Whoever . . . 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. . . ." 18 U.S.C. 1030(a)(3)(emphasis added).

[65] "(e) As used in this section . . . (7) the term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5," 18 U.S.C. 1030(e)(7).

[66] "As used in this title: The term 'department' means one of the executive departments enumerated in section 1 [now section 1010] of Title 5, unless the context shows that such term was intended to describe the executive, legislative, or judicial branches of the government. The term 'agency' includes any department, independent establishment, commission, administration, authority, board or bureau of the United States or any corporation in which the United States has a proprietary interest, unless the context shows that such term was intended to be used in a more limited sense," 18 U.S.C. 6.

[67] "(e) As used in this section. . . (4) the term financial institution' means – (A) an institution with deposits insured by the Federal Deposit Insurance Corporation; (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank; (C) a credit union with accounts insured by the National Credit Union Administration; (D) a member of the Federal home loan bank system and any home loan bank; (E) any institution of the Farm Credit System under the Farm Credit Act of 1971; (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; (G) the Securities Investor Protection Corporation; (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); (I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act," 18 U.S.C. 1030(e)(4).

[68] "As used in this title, the term 'financial institution' means – (1) an insured depository institution (as defined in section 3(c)(2) of the Federal Deposit Insurance Act); (2) a credit union with accounts insured by the National Credit Union Share Insurance Fund; (3) a Federal home loan bank or a member, as defined in section 2 of the Federal Home Loan Bank Act (12 U.S.C. 1422), of the Federal home loan bank system; (4) a System institution of the Farm Credit System, as defined in section 5.35(3) of the Farm Credit Act of 1971; (5) a small business investment company, as defined in section 103 of the Small Business Investment Act of 1958 (15 U.S.C. 662); (6) a depository institution holding company (as defined in section 3(w)(1) of the Federal Deposit Insurance Act; (7) a Federal Reserve bank or a member bank of the Federal Reserve System; (8) an organization operating under section 25 or section 25(a) of the Federal Reserve Act; or (9) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978)," 18 U.S.C. 20.

Penalties.

The paragraph punishes causing damage recklessly or intentionally more severely than causing damage without necessarily intending to do. Causing damage, without necessarily intending to do so, by intentionally gaining access, or attempting to gain access, to a protected computer is punishable by imprisonment of not more than 1 year (not more than 10 years for a second or subsequent offense) and/or a fine of not more than $100,000 ($200,000 for organizations)(not more than $250,000/$500,0,00 for a second or subsequent offense) 18 U.S.C. 1030(c)(2)(A), (c)(3)(B); 18 U.S.C. 3571.[69] *Recklessly* causing damage by intentionally gaining access, or attempting to gain access, to a protected computer is punishable by imprisonment for not more than *5* years (not more than 20 years for a second or subsequent offense) and/or a fine of not more than $250,000 (not more than $500,000 for an organization), 18 U.S.C. 1030(c)(4)(B); 18 U.S.C. 3571. *Intentionally* causing damage through a knowing transmission to a protected computer is punishable by imprisonment for not more than *10* years (not more than 20 years for a second or subsequent offense) and/or a fine of not more than $250,000 (not more than $500,000 for an organization), 18 U.S.C. 1030(c)(4)(A); 18 U.S.C. 3571. An offender who knowingly or recklessly causes or attempts to cause serious bodily injury or death by knowingly causing an intentionally damaging transmission to a protected computer is punishable by imprisonment for not more than of 20 years (any term of years or life if death results) and/or fine of $250,000 ($500,000 for an organization), 18 U.S.C. 1030(c)(5), 18 U.S.C. 3571.[70]

The same sentencing guideline applies to violations of paragraph 1030(a)(5)(causing damage) as covers paragraph 1030(a)(2)(unauthorized access with the acquisition of information), U.S.S.G. §2B1.1: a base offense level of 6; an increase of 2 offense levels when the victimized computer is used in the critical infrastructure or by a government entity of national security, defense, or criminal justice purposes (an increase of 6 offense levels and a final offense level of at least

---

[69] Section 805(c) of the Antiterrorism and Effective Death Penalty Act of 1996, 110 Stat. 1305, instructed the United States Sentencing Commission to adjust the applicable sentencing guidelines so that any violation of paragraph 1030(a)(5) would be punishable by imprisonment for not less than six months. The Commission did so with respect to any violations occurring on or after November 1, 1997, U.S.S.G. §2b1.3(d), 62 *Fed.Reg.* 26620-621 (May 14, 1997). Section 814(f) of the USA PATRIOT Act, 28 U.S.C. 994 note, instructed the Commission to amend the Guidelines to ensure the imposition of appropriate penalties "without regard to any mandatory minimum term of imprisonment." For a criticism of these increased penalties, see Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECHNOLOGY LAW JOURNAL 909, 934 (2003).

[70] The Homeland Security Act added this provision; the USA PATRIOT Act increased the penalty for second or subsequent offenses from imprisonment for not more than 10 to imprisonment for not more than 20 years, and the penalty for intentionally causing damage to a protected computer through a knowing transmission from imprisonment for not more than 5 years to imprisonment for not more than 10 years. The applicable Sentencing Guideline sets the sentencing ranges for paragraph 1030(a)(5) violations according to the amount of damage done, the number of victims, and any risk of death or serious injury, U.S.S.G. §2B1.1.

24 when the offense involves a substantial disruption of a critical infrastructure); and of greater significance here an increase of from 2 to 30 levels depending upon the extent of any damage caused as well as an increase of from 2 to 6 levels depending upon the number of victims involved. In addition, for violations of 1030(a)(5)(A)(i), there is an increase of four levels.

Victims of a violation of paragraph 1030(a)(5) or any violation of subsection 1030(a) resulting in the requisite harm have a cause of action for compensatory damages and equitable relief if suit is brought within 2 years.[71] Damages to medical records, or damage causing physical injury or endangering public safety may also subject the offender to "compensatory" damages beyond "economic" damages – a difference that may entitle a victim to pecuniary damages as well as damages for pain and suffering but probably not exemplary damages.[72] Damages caused by a simply knowing violation of paragraph 1030(a)(5) (as opposed to reckless and intentional violations) are limited to economic damages.

Victims are described as "any person who suffers loss or damage by reason of a violation of this section," but until recently there was no specific definition of the term "person" in either section 1030 or in the definitions applicable to title 18

---

[71] "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware,"18 U.S.C. 1030(g).

The damages described in clauses 1030(a)(5)(B)(i) through (v) are: "(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security." Under section 1030(g) the plaintiffs must show actual "quantifiable" damage. See e.g. *Pearl Investments v. Standard I/O*, 257 F.Supp.2d 326, 349 (D.Me. 2003) (slowing of system's speed and operation did not meet monetary threshold for civil action under 1030(g)).

[72] Black's defines compensatory damages as those damages "sufficient in amount to indemnify the injured person for the loss suffered," BLACK'S LAW DICTIONARY, *Damages* (8th ed. 2004). It recognizes no separate definition for "economic damages," but the term is defined elsewhere in title 18 of the United States Code as "the replacement costs of lost or damaged property or records, the cost of repeating an interrupted or invalidated experiment, or the loss of profits," 18 U.S.C. 43(d)(3).

generally.[73] The legislative history offered no further edification and the provision has yet to be construed by the courts. "Person" could mean individuals, or individuals and other legal entities including governmental entities, or individuals and other legal entities but not including governmental entities. Creditable arguments can be made for each of the possible definitions, but the fact that Congress elected to use the term "person" to mean only individuals in paragraph 1030(a)(7)(extortionate threats)[74] might seem to favor a similar interpretation in subsection 1030(g). The USA PATRIOT Act resolved the question and answered several others.

First, it supplied a definition of person – "the term 'person' means any individual, firm, corporation, educational institution, governmental entity, or legal or other entity," 18 U.S.C. 1030(e)(12). Then, it added an equally generous definition of the kinds of losses that might give raise to civil liability – "the term 'loss' means 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," 18 U.S.C. 1030(e)(11). Finally, it made clear that subsection 1030(g) does not create a cause of action for loss or damage attributable to "the negligent design or manufacture of computer hardware, computer software, or firmware," 18 U.S.C. 1030(g).[75]

Other Crimes.

Attempt, Conspiracy, and Complicity.

The same general observations concerning attempt, conspiracy and aiding and abetting noted for the simple trespass paragraph apply here. It is a separate crime to attempt to violate paragraph 1030(a)(5) or any of the other paragraphs of subsection

---

[73] Who can be a victim has also been broadly defined by the courts, and rights to civil remedies under the statute have been extended to third parties. The court in *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004), emphasized that the statute extends a civil remedy to *any* person who suffers loss or damage, thus "[i]ndividuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it."

[74] "Whoever. . . (7) with intent to extort from any *person, firm, association, educational institution, financial institution, government entity, or other legal entity*, any money or other thing of value . . ." 18 U.S.C. 1030(a)(7)(emphasis added)(the 2002 amendments struck out "firm, association, educational institution, financial institution, government entity, or other legal entity").

[75] For some of the difficulties associated with possible manufacturer liability under subsection 1030(g) prior to amendment see, *In re America Online, Inc.*, 168 F.Supp.2d 1359 (S.D.Fla. 2001)(allegations that provider's software damaged customers' computers); *Thurmond v. Compaq Computer Corp.*, 171 F.Supp.2d 667 (E.D. Tex. 2001)(floppy disk controllers that allegedly corrupted or destroyed data); *Hayes v. Packard Bell NEC, Inc.*, 193 F.Supp.2d 910 (E.D.Tex. 2001)(same); *Christian v. Sony Corp. of America*, 152 F.Supp.2d 1184 (D.Minn. 2001)(same).

1030(a), 18 U.S.C. 1030(b). Those who attempt to violate or who aid and abet the violation of another are subject to the same penalties as those commit the substantive offense, 18 U.S.C. 1030(c), 2. The same is true of conspiracies except that conspiracy to commit a felony carries a 5 year maximum of imprisonment, 18 U.S.C. 371.

Although more likely to be relevant in the context of paragraph 1030(a)(4)(fraud) discussed below at greater length, certain violations of paragraph 1030(a)(5) can provide the basis for a prosecution under federal racketeering laws, 18 U.S.C. 1961-1965, and consequently under federal money laundering statutes, 18 U.S.C. 1956. The USA PATRIOT Act enlarged the definition of federal crimes of terrorism, 18 U.S.C. 2332b(g)(5)(B), to include intentionally damaging a protected computer if the offense involves either impairing medical care, causing physical injury, threatening public health or safety, or damaging a governmental justice, national defense, or national security computer system.[76]

It then enlarged the RICO predicate offense list to include "any act that is indictable under any provision listed in section 2332b(g)(5)(B)," 18 U.S.C. 1961(1)(G). Among other things, RICO outlaws the patterned commission of predicate offenses ("racketeering activities") in order to acquire or conduct the affairs of an enterprise whose activities affect interstate or foreign commerce.[77] Crimes on its predicate offense list are also "specified unlawful activities" for purposes of 18 U.S.C. 1956 and 1957 and thus may serve as the basis for a prosecution under the money laundering provisions of those sections, 18 U.S.C. 1956(c)(7)(A), 1957(f)(3). Section 1956 outlaws, among other things, conducting a financial transaction using the proceeds of a specified unlawful activity in order to promote such an activity or to launder the proceeds of such an activity.[78] Section 1957 outlaws financial

---

[76] 18 U.S.C. 2332b(g)(5)(B)(i)("the term 'federal crime of terrorism means' means an offense that . . . (B) is a violation of – (i) section . . . 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through (v). . . of this title").

[77] "(b) It shall be unlawful for any person through a pattern of racketeering activity or through collection of an unlawful debt to acquire or maintain, directly or indirectly, any interest in or control of any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce.

"(c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt," 18 U.S.C. 1962(b), (c).

[78] "Whoever, with the intent– (A) to promote the carrying on of specified unlawful activity; (B) to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity; or (C) to avoid a transaction reporting requirement under State or Federal law, conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity, shall be fined under this title or imprisoned for not more than 20 years, or both. . . ." 18 U.S.C. 1956(a)(3).

transactions in the proceeds of specified unlawful activities involving more than $10,000.[79]

Damage or destruction of federal property.

There are more than a few other federal statutes that might be implicated by damage or destruction of federal property, of the property of financial institutions, or of property used in interstate or foreign commerce. The principal uncertainty is whether these general statutes can be applied to protect intangible property, like information in computer storage. Even if computer-stored data is considered tangible property (electronic files rather than paper files), several statutes that outlaw damage or destruction may be unavailable because they either call for a specific means of destruction – destruction by fire or explosives – or because they protect a particular kind of property – timber or buildings.[80]

Destruction of government records. It is a federal crime for anyone to unlawfully "conceal, remove, mutilate, obliterate, or destroy . . . any record, proceeding, map, book, paper, document, or other thing, filed or deposited with . . . any judicial or public officer of the United States."[81] The damage or destruction of

---

[79] 18 U.S.C. 1957(a) states, "Whoever, in any of the circumstances set forth in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity, shall be punished as provided in subsection (b). . . .

"(d) The circumstances referred to in subsection (a) are – (1) that the offense under this section takes place in the United States or in the special maritime and territorial jurisdiction of the United States; or (2) that the offense under this section takes place outside the United States and such special jurisdiction, but the defendant is a United States person (as defined in section 3077 of this title, but excluding the class described in paragraph (2)(D) of such section)").

[80] "(f)(1) Whoever maliciously damages or destroys, or attempts to damage or destroy, *by means of fire or an explosive*, any building, vehicle, or other personal or real property in whole or in part owned or possessed by, or leased to, the United States, or any department or agency thereof, shall be imprisoned for not less than 5 years and not more than 20 years, fined under this title, or both.

"(2) Whoever engages in conduct prohibited by this subsection, and as a result of such conduct, directly or proximately causes personal injury or creates a substantial risk of injury to any person, including any public safety officer performing duties, shall be imprisoned for not less than 7 years and not more than 40 years, fined under this title, or both.

"(3) Whoever engages in conduct prohibited by this subsection, and as a result of such conduct directly or proximately causes the death of any person, including any public safety officer performing duties, shall be subject to the death penalty, or imprisoned for not less than 20 years or for life, fined under this title, or both," 18 U.S.C. 844(f)(emphasis added).

"Whoever unlawfully cuts, or wantonly injures or destroys any tree growing, standing, or being upon any land of the United States . . . shall be fined under this title or imprisoned not more than one year, or both," 18 U.S.C. 1853.

[81] "(a) Whoever willfully and unlawfully conceals, removes, mutilates, obliterates, or destroys, or attempts to do so, or, with intent to do so takes and carries away any record, proceeding, map, book, paper, document, or other thing, filed or deposited with any clerk or officer of any court of the United States, or in any public office, or with any judicial or public officer of the United States, shall be fined under this title or imprisoned not more than

government, computer-stored records will fall within the coverage of section 2071 only if it can meet each of the action (obliterate or destroy), object (any record or other thing) and place (filled with a federal judicial or public officer) tests.

The phrase "conceal, remove, mutilate, obliterate, or destroy" may lend itself to the argument that it extends to destruction or complete inaccessibility, but perhaps not to less than totally destructive damage, of computerized records. Electronic destruction seems to fit under either "obliterate" ("to make undecipherable by obscuring")[82] or "destroy". Absent obliteration or destruction, the section may be thought to protect only tangibles, since the word "mutilate" has obvious physical connotations. Yet one court among the few to construe section 2071 held that it did not prohibit photocopying of government records – not because that would constitute the removal of an intangible (information), but because the statute was designed to prevent "any conduct which deprives the Government of the use of its documents."[83]

The phrase "any record, proceeding, map, book, paper, document, or other thing, filed or deposited with" would seem to cover any "thing" capable of being "filed or deposited". In these days of "electronic filing"[84] any contention that federal computer records do not fit the phrase seems untenable.

The final requirement might appear to protect only those records based on deposits with federal court or administrative officials, but the scant case law available suggests coverage extends to any record maintained by the government.[85]

---

three years, or both.

"(b) Whoever, having the custody of any such record, proceeding, map, book, document, paper, or other thing, willfully and unlawfully conceals, removes, mutilates, obliterates, falsifies, or destroys the same, shall be fined under this title or imprisoned not more than three years, or both; and shall forfeit his office and be disqualified from holding any office under the United States. As used in this subsection, the term "office" does not include the office held by any person as a retired officer of the Armed Forces of the United States," 18 U.S.C. 2071.

[82] MERRIAM WEBSTER'S COLLEGIATE DICTIONARY, 802 (10th ed. 1996).

[83] *United States v. Rosner*, 352 F.Supp. 915, 919 (S.D.N.Y. 1972).

[84] See e.g., 26 U.S.C. 6011(e)(1)("The Secretary shall prescribe regulations providing standards for determining which returns must be filed on magnetic media or in other machine-readable form."); IRS Pub. 1345 (2001); 26 C.F.R. §301.7502-1(d) ("Electronically filed documents– (1) In general. A document filed electronically with an electronic return transmitter... in the manner and time prescribed by the Commissioner is deemed to be filed on the date of the electronic postmark ...given by the authorized electronic return transmitter. Thus, if the electronic postmark is timely, the document is considered filed timely although it is received by the agency, officer, or office after the last date, or the last day of the period, prescribed for filing such document.")

[85] *United States v. Lang*, 364 F.3d 1210 (10th Cir. 2004)(copy of officially filed court document), rem'd for reconsideration in light of *United States v. Booker*, 125 S.Ct. 986 (2005), reinstated in part, 405 F.3d 1060 (10th Cir. 2005);*United States v. Poindexter*, 725 F.Supp. 13, 19 (D.D.C. 1989)(National Security Council records); *Coplon v. United States*, 191 F.2d 749 (D.C.Cir. 1951)(FBI counter-intelligence reports).

Violations of section 2071 are punishable by imprisonment for not more than 3 years and/or a fine of not more than $250,000, or both fine and imprisonment, 18 U.S.C. 2071, 3571.

Destruction of federal property. It is a federal crime to "willfully injure or commit any depredation against any property of the United States. . . ."[86] Although an offender must be shown to have to injure or depredate property, the government need not show that the defendant knew the property belonged to the government.[87] The federal courts have permitted prosecution under section 1361 of a defendant who used a hammer and drill to destroy a federal computer.[88] There are no reported cases in which section 1361 was used to prosecute electronic computer abuse for damaging federal property, and federal authorities used an earlier version of the computer abuse statute, section 1030, to prosecute one of the first cases of electronic computer abuse resulting in damage.[89]

Damage or destruction of federal property is punishable by imprisonment for not more than 10 years and/or a fine of not more than $250,000 (or not more than 1 year and/or a fine of not more than $100,000 if the damage causes amounts to $1,000 or less and no one dies as a result of the offense), 18 U.S.C. 1361; 18 U.S.C. 3571.

Destruction of federal communications systems. Willful or malicious interference or disruption "in any way" with any communications system owned by the United States or used by the United States for military or civil defense purposes is punishable by imprisonment for not more than 10 years and/or a fine of not more

---

[86] "Whoever willfully injures or commits any depredation against any property of the United States, or of any department or agency thereof, or any property which has been or is being manufactured or constructed for the United States, or any department or agency thereof, or attempts to commit any of the foregoing offenses, shall be punished as follows:

"If the damage or attempted damage to such property exceeds the sum of $1,000, by a fine under this title or imprisonment for not more than ten years, or both; if the damage or attempted damage to such property does not exceed the sum of $1,000, by a fine under this title or by imprisonment for not more than one year, or both." 18 U.S.C. 1361.

[87] *United States v. Urfer* 287 F.3d 663, 666 (7th Cir. 2002); but see, *United States v. Bangert*, 645 F.2d 1297, 1305 (8th Cir. 1981).

[88] *United States v. Komisaruk*, 885 F.2d 490 (9th Cir. 1989).

[89] *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991).

than $250,000.[90] The language of section 1362 leaves little room for any contention that it does not apply to computer abuse aimed at federal communications facilities.

Damage or destruction of financial institution property.

A handful of federal statutes protect financial institutions from theft in one form or another, but not property damage or destruction. Section 1030 appears to be the only statute that includes a specific provision designed to protect the property of financial institutions from damage or destruction. As with *Morris*, a defendant prosecuted under an earlier version of paragraph 1030(a)(5) questioned what level of intent was required with respect to the damage caused.[91]

Damage or destruction to property in interstate commerce.

Transportation. The federal statutes, other than paragraph 1030(a)(5), most likely to cover the computerized damage or destruction to property in interstate commerce involve transportation. Each of the provisions that proscribe interference with air, motor, rail and sea transportation appear to have been drafted with sufficient breadth to reach damage or destruction of at least some of the computer systems incidental to those transportation facilities.

For example, the provisions applicable to the destruction of aircraft and aircraft facilities penalize anyone who "damages, destroys, or disables any air navigation facility . . . if such . . . damaging, destroying, [or] disabling . . . is likely to endanger the safety of any such aircraft," 18 U.S.C. 32(a)(3).[92] This would presumably protect

---

[90] 18 U.S.C. 1362; 18 U.S.C. 3571. Section 1362 provides in full that: "Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both

"In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defense functions of the United States."

[91] *United States v. Sablan*, 92 F.3d 865, 867-69 (9th Cir. 1996). As originally worded, the paragraph penalized anyone who "intentionally accesse[d] a Federal interstate computer . . . and by means of . . . such conduct . . . damage[d]. . . information in such . . . computer," 18 U.S.C. 1030(a)(5)(1988 ed.). Defendants in *Morris* and *Sablan* argued unsuccessfully that the government was required to show that offender had both intentionally accessed a federal computer *and* had intentionally damaged information in the computer. The current wording eliminates the grounds for such contentions.

[92] Violations, attempted violations, and conspiracies to violate the provisions of section 32 are all punishable by imprisonment for not more than 20 years and/or a fine of not more than $250,000, 18 U.S.C. 32(a); 18 U.S.C. 3571; violations that result in death are punishable by

air traffic control systems, but not computerized passenger information, i.e. gridlock is not proscribed unless it "endanger[s] the safety" of air travel.

---

life imprisonment or death, 18 U.S.C. 34. The full text of 18 U.S.C. 32 is as follows: "(a) Whoever willfully –

"(1) sets fire to, damages, destroys, disables, or wrecks any aircraft in the special aircraft jurisdiction of the United States or any civil aircraft used, operated, or employed in interstate, overseas, or foreign air commerce;

"(2) places or causes to be placed a destructive device or substance in, upon, or in proximity to, or otherwise makes or causes to be made unworkable or unusable or hazardous to work or use, any such aircraft, or any part or other materials used or intended to be used in connection with the operation of such aircraft, if such placing or causing to be placed or such making or causing to be made is likely to endanger the safety of any such aircraft;

"(3) sets fire to, damages, destroys, or disables any air navigation facility, or interferes by force or violence with the operation of such facility, if such fire, damaging, destroying, disabling, or interfering is likely to endanger the safety of any such aircraft in flight;

"(4) with the intent to damage, destroy, or disable any such aircraft, sets fire to, damages, destroys, or disables or places a destructive device or substance in, upon, or in proximity to, any appliance or structure, ramp, landing area, property, machine, or apparatus, or any facility or other material used, or intended to be used, in connection with the operation, maintenance, loading, unloading or storage of any such aircraft or any cargo carried or intended to be carried on any such aircraft;

"(5) performs an act of violence against or incapacitates any individual on any such aircraft, if such act of violence or incapacitation is likely to endanger the safety of such aircraft;

"(6) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safety of any such aircraft in flight; or

"(7) attempts or conspires to do anything prohibited under paragraphs (1) through (6) of this subsection;

shall be fined under this title or imprisoned not more than twenty years or both.

"(b) Whoever willfully -- (1) performs an act of violence against any individual on board any civil aircraft registered in a country other than the United States while such aircraft is in flight, if such act is likely to endanger the safety of that aircraft;

"(2) destroys a civil aircraft registered in a country other than the United States while such aircraft is in service or causes damage to such an aircraft which renders that aircraft incapable of flight or which is likely to endanger that aircraft's safety in flight;

"(3) places or causes to be placed on a civil aircraft registered in a country other than the United States while such aircraft is in service, a device or substance which is likely to destroy that aircraft, or to cause damage to that aircraft which renders that aircraft incapable of flight or which is likely to endanger that aircraft's safety in flight; or

"(4) attempts or conspires to commit an offense described in paragraphs (1) through (3) of this subsection;

shall be fined under this title or imprisoned not more than twenty years, or both. There is jurisdiction over an offense under this subsection if a national of the United States was on board, or would have been on board, the aircraft; an offender is a national of the United States; or an offender is afterwards found in the United States. For purposes of this subsection, the term "national of the United States" has the meaning prescribed in section 101(a)(22) of the Immigration and Nationality Act.

"(c) Whoever willfully imparts or conveys any threat to do an act which would violate any of paragraphs (1) through (5) of subsection (a) or any of paragraphs (1) through (3) of subsection (b) of this section, with an apparent determination and will to carry the threat into execution shall be fined under this title or imprisoned not more than five years, or both."

The language of the provisions outlawing interference with maritime navigation are strikingly comparable: "a person who unlawfully and intentionally . . . destroys or seriously damages maritime navigational facilities or serious interferes with their operation, is such act is like to endanger the safe navigation of a ship" or attempts or conspires to do so is punishable by imprisonment for not more than 20 years and/or a fine of not more than $250,000, or if death results form commission of the offense, by imprisonment for life or death.[93] Federal jurisdiction for prosecution exists if the

---

[93] 18 U.S.C. 2280; 18 U.S.C. 3571. Section 2280 provides in full: "(a)(1) In general.– A person who unlawfully and intentionally – (A) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; (B) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; (C) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship; (D) places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; (E) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if such act is likely to endanger the safe navigation of a ship; (F) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safe navigation of a ship; (G) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (F); or (H) attempts or conspires to do any act prohibited under subparagraphs (A) through (G), shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be punished by death or imprisoned for any term of years or for life.

"(2) Threat to navigation. – A person who threatens to do any act prohibited under paragraph (1) (B), (C) or (E), with apparent determination and will to carry the threat into execution, if the threatened act is likely to endanger the safe navigation of the ship in question, shall be fined under this title, imprisoned not more than 5 years, or both.

"(b) Jurisdiction.–There is jurisdiction over the activity prohibited in subsection (a) – (1) in the case of a covered ship, if – (A) such activity is committed – (i) against or on board a ship flying the flag of the United States at the time the prohibited activity is committed; (ii) in the United States; or (iii) by a national of the United States or by a stateless person whose habitual residence is in the United States; (B) during the commission of such activity, a national of the United States is seized, threatened, injured or killed; or (C) the offender is later found in the United States after such activity is committed;

"(2) in the case of a ship navigating or scheduled to navigate solely within the territorial sea or internal waters of a country other than the United States, if the offender is later found in the United States after such activity is committed; and

"(3) in the case of any vessel, if such activity is committed in an attempt to compel the United States to do or abstain from doing any act.

"(c) Bar to prosecution. – It is a bar to Federal prosecution under subsection (a) for conduct that occurred within the United States that the conduct involved was during or in relation to a labor dispute, and such conduct is prohibited as a felony under the law of the State in which it was committed. For purposes of this section, the term "labor dispute" has the meaning set forth in section 2(c) of the Norris-LaGuardia Act, as amended (29 U.S.C. 113(c))

"(d) Delivery of suspected offender.– The master of a covered ship flying the flag of the United States who has reasonable grounds to believe that there is on board that ship any person who has committed an offense under Article 3 of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation may deliver such person to the authorities of a State Party to that Convention. Before delivering such person to the

offense occurs within American territorial waters, if the vessel or vessels engaged are of American registry, or if committed by American or by someone later found in this country, 18 U.S.C. 2280(b).

Similarly, "whoever. . . makes any structure, property, appurtenance unworkable or unusable or hazardous to work or use, with the intent to derail, disable, or wreck a train, engine, motor unit, or car used, operated, or employed in interstate or foreign commerce" is punishable by imprisonment for not more than 20 years and/or a fine of not more than $250,000, if death results from commission of the offense, by imprisonment for life or death.[94] Once again, computer abuse that targets rail traffic

---

authorities of another country, the master shall notify in an appropriate manner the Attorney General of the United States of the alleged offense and await instructions from the Attorney General as to what action to take. When delivering the person to a country which is a State Party to the Convention, the master shall, whenever practicable, and if possible before entering the territorial sea of such country, notify the authorities of such country of the master's intention to deliver such person and the reasons therefor. If the master delivers such person, the master shall furnish to the authorities of such country the evidence in the master's possession that pertains to the alleged offense.

"(e) Definitions.– In this section – 'covered ship' means a ship that is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single country or a lateral limit of that country's territorial sea with an adjacent country; 'national of the United States' has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22)); 'territorial sea of the United States' means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law; 'ship' means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles or any other floating craft, but does not include a warship, a ship owned or operated by a government when being used as a naval auxiliary or for customs or police purposes, or a ship which has been withdrawn from navigation or laid up; 'United States,' when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands and all territories and possessions of the United States."

[94] 18 U.S.C. 1992; 18 U.S.C. 3571. The full text of 18 U.S.C. 1992 provides: "(a) Whoever willfully derails, disables, or wrecks any train, engine, motor unit, or car used, operated, or employed in interstate or foreign commerce by any railroad; or Whoever willfully sets fire to, or places any explosive substance on or near, or undermines any tunnel, bridge, viaduct, trestle, track, signal, station, depot, warehouse, terminal, or any other way, structure, property, or appurtenance used in the operation of any such railroad in interstate or foreign commerce, or otherwise makes any such tunnel, bridge, viaduct, trestle, track, signal, station, depot, warehouse, terminal, or any other way, structure, property, or appurtenance unworkable or unusable or hazardous to work or use, with the intent to derail, disable, or wreck a train, engine, motor unit, or car used, operated, or employed in interstate or foreign commerce; or Whoever willfully attempts to do any of the aforesaid acts or things – Shall be fined under this title or imprisoned not more than twenty years, or both.

"(b) Whoever is convicted of a violation of subsection (a) that has resulted in the death of any person, shall be subject also to the death penalty or to imprisonment for life.

"Whoever is convicted of any such violation involving a train that, at the time the violation occurred, carried high-level radioactive waste (as that term is defined in section 2(12) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101(12))) or spent nuclear fuel (as that term is defined in section 2(23) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101(23))), shall be fined under this title and imprisoned for any term or years not less than

control is almost certainly covered; computer abuse that targets ticket control is almost certainly not.

The language of the federal law outlawing the destruction of motor vehicle facilities seems only slightly more modest, for it extends to anyone who "with a reckless disregard for the safety of human life," willfully "damages, destroys. . . tampers with," or otherwise makes "unworkable, unusable, or hazardous to work or use" any "facility used in the operation of, or in support of the operation of, motor vehicles engaged in interstate or foreign commerce," 18 U.S.C. 33(a).[95] Computer

---

30, or for life.

"(c) A person who conspires to commit any offense defined in this section shall be subject to the same penalties (other than them penalty of death) as the penalties prescribed for the offense, the commission of which was the object of the conspiracy."

The statute prohibiting terrorist attacks on mass transportation systems contains a similar proscription: "Whoever willfully . . . (4) removes appurtenances from, damages, or otherwise impairs the operation of a mass transportation signal system, including a train control system, centralized dispatching system, or rail grade crossing warning signal without authorization from the mass transportation provider . . . or (8) attempts, threatens, or conspires to do any of the aforesaid acts, shall be fined under this title or imprisoned not more than twenty years, or both, if such act is committed, or in the case of a threat or conspiracy such act would be committed, on, against, or affecting a mass transportation provider engaged in or affecting interstate or foreign commerce, or if in the course of committing such act, that person travels or communicates across a State line in order to commit such act, or transports materials across a State line in aid of the commission of such act." 18 U.S.C. 1993(a)(4), (8).

[95] Violations are punishable by imprisonment for not more than 20 years and/or a fine of not more than $250,000 or, if death results from commission of the offense, by imprisonment for life or death, 18 U.S.C. 33(a); 18 U.S.C. 34; 18 U.S.C. 3571.

Section 18 U.S.C. 33 states in full: "(a) Whoever willfully, with intent to endanger the safety of any person on board or anyone who he believes will board the same, or with a reckless disregard for the safety of human life, damages, disables, destroys, tampers with, or places or causes to be placed any explosive or other destructive substance in, upon, or in proximity to, any motor vehicle which is used, operated, or employed in interstate or foreign commerce, or its cargo or material used or intended to be used in connection with its operation; or

"Whoever willfully, with like intent, damages, disables, destroys, sets fire to, tampers with, or places or causes to be placed any explosive or other destructive substance in, upon, or in proximity to any garage, terminal, structure, supply, or facility used in the operation of, or in support of the operation of, motor vehicles engaged in interstate or foreign commerce or otherwise makes or causes such property to be made unworkable, unusable, or hazardous to work or use; or

"Whoever, with like intent, willfully disables or incapacitates any driver or person employed in connection with the operation or maintenance of the motor vehicle, or in any way lessens the ability of such person to perform his duties as such; or

"Whoever willfully attempts to do any of the aforesaid acts --

shall be fined under this title or imprisoned not more than twenty years, or both.

"(b) Whoever is convicted of a violation of subsection (a) involving a motor vehicle that, at the time the violation occurred, carried high-level radioactive waste (as that term is defined in section 2(12) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101(12))) or spent nuclear fuel (as that term is defined in section 2(23) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101(23))), shall be fined under this title and imprisoned for any

abuse that damages or destroys motor traffic control systems in a manner threatening to human safety would seem to fall within the reach of section 33.

Other crimes. Other federal crimes that might be implicated by damaging computer systems used in interstate or foreign commerce include those that cover damage to an energy facility[96] or proscribe interference with the operation of a communications or weather satellite.[97] Most of the states also outlaw damaging computer equipment, software, or systems.[98]

---

term of years not less than 30, or for life.

[96] "(a) Whoever knowingly and willfully damages or attempts to damage the property of an energy facility in an amount that in fact exceeds or would if the attempted offense had been completed have exceeded $100,000, or damages or attempts to damage the property of an energy facility in any amount and causes or attempts to cause a significant interruption or impairment of a function of an energy facility, shall be punishable by a fine under this title or imprisonment for not more than 20 years, or both.

"(b) Whoever knowingly and willfully damages or attempts to damage the property of an energy facility in an amount that in fact exceeds or would if the attempted offense had been completed have exceeded $5,000 shall be punishable by a fine under this title, or imprisonment for not more than five years, or both.

"(c) For purposes of this section, the term 'energy facility' means a facility that is involved in the production, storage, transmission, or distribution of electricity, fuel, or another form or source of energy, or research, development, or demonstration facilities relating thereto, regardless of whether such facility is still under construction or is otherwise not functioning, except a facility subject to the jurisdiction, administration, or in the custody of the Nuclear Regulatory Commission or an interstate gas pipeline facility as defined in section 60101 of title 49.

"(d) Whoever is convicted of a violation of subsection (a) or (b) that has resulted in the death of any person shall be subject to imprisonment for any term of years or life," 18 U.S.C. 1366.

[97] "(a) Whoever, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite transmission shall be fined in accordance with this title or imprisoned not more than ten years or both," 18 U.S.C. 1367.

[98] See e.g., ALA.CODE 1975 §§13A-8-102, 13A-8-103; ALASKA STAT. §11.46.740; ARIZ.REV. STAT.ANN. §13-2316; ARK.CODEANN. §5-41-202; CAL.PENAL CODE §502; COLO.REV. STAT.ANN. §18-5.5-102; CONN.GEN.STAT.ANN. §53a-251; DEL.CODEANN. tit.11 §936; FLA. STAT.ANN. §§815.04, 815.06; GA.CODEANN. §16-9-93; HAWAII REV.STAT. §§708-892, 892.5; IDAHO CODE §18-2202; ILL.COMP.LAWS ANN. ch.720 ¶5, §§16D-3, 16D-4; IND.CODE ANN. §35-43-1-4; IOWA CODE ANN. §§716.1, 716.6B; KAN.STAT.ANN. §21-3755; KY.REV.STAT.ANN. §434.845, et seq.; LA.REV.STAT.ANN. §§14: 73.3, 73.4, 73.7; ME. REV.STAT.ANN. tit.17-A §433; MD.CRIM.CODE ANN. §7-302; MASS.GEN.LAWS ANN. Ch.266, §127; MICH.COMP.LAWS ANN. §752.795; MINN. STAT.ANN. §609.88; MISS.CODEANN. §97-45-7, 9; MO.ANN.STAT. §§569.095 to 569.099; MONT.CODE ANN. §45-6-311; NEB.REV.STAT. §28-1345; NEV.REV.STAT. 205.4765; N.H. REV.STAT.ANN. §638:17;N.J.STAT.ANN. §§2C:20-25, 2A:38A-3; N.MEX.STAT.ANN. §30-45-4; N.Y.PENAL LAW §§156.10 to 156.27; N.C.GEN.STAT. §§14-455, 458; N.D. CENT. CODE §12.1-06.1-08; OKLA.STAT.ANN. tit.21 §1953; ORE.REV.STAT. §164.377; PA. STAT. ANN. tit.18 §1711, 1715, 1716; R.I.GEN.LAWS §11-52-4.1; S.C.CODE ANN. §16-16-20; S.D.COD. LAWS §43-43B-1; TENN.CODE ANN. §39-14-602; TEX.PENAL CODE ANN. §33.02; UTAH CODE ANN. §76-6-703; VT.STAT.ANN. tit.13 §4103; VA.CODE. §18.2-152.4;

Computer Fraud
18 U.S.C. 1030(a)(4)

> *(a) 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.*

Paragraph 1030(a)(4) outlaws fraud by computer intrusion. Its elements consist of:

- knowingly and with intent to defraud;
- accessing a protected computer without authorization, or exceeding authorization;
- thereby furthering a fraud and obtaining anything of value other than a minimal amount of computer time (more than $5,000 over the course of a year).

Jurisdiction.

Paragraph 1030(a)(4) outlaws fraud against "protected computers," i.e., computers used in interstate or foreign commerce, 18 U.S.C. 1030(e)(2)(B), those used by or for "the United States Government," or those used by or for a financial institution, 18 U.S.C. 1030(e)(2)(A). As noted earlier, there may be some real doubt whether in doing so it reaches computers of the legislative and judicial branches or of the independent federal agencies, or whether it shields only those within the executive branch. The wording of some of the paragraphs of section 1030 clearly anticipates expansive coverage. Having declined to take advantage of those terms of art with respect to paragraph 1030(a)(4), should Congress be presumed to have intended a more limited reach? As noted earlier, the counterpoint is that in one paragraph of section 1030, Congress uses the phrase "Government of the United States" interchangeably with the more expansive phrase "department or agency of the United States," 18 U.S.C. 1030(a)(3). If the terms are interchangeable at one point within the section should they not be construed as interchangeable through out?

The Committee reports indicate that Congress understood the phrase "used in interstate or foreign commerce" to be the equivalent of "affecting interstate or foreign commerce," S.Rep.No. 104-357 at 10 (1996).

WASH.REV.CODE ANN. §§9A.48.070 to 9A.48.100; W.VA.CODE ANN. §61-3C-7; WIS.STAT.ANN. §943.70; WYO.STAT. §§6-3-501 to 6-3-504.

Intent.

Paragraph 1030(a)(4) was proposed as part of the original statute in 1984, H.R.Rep.No. 98-894 at 27 (1984), but only enacted with the 1986 amendments, Pub.L.No. 99-474, 100 Stat. 1213 (1986), 18 U.S.C. 1030 (1986 Supp.). The reports accompanying the 1986 amendments note that the intent element – "knowingly and with intent to defraud" – "is the same standard used for 18 U.S.C. 1029 relating to credit card fraud," S.Rep.No. 99-432 at 10 (1986); H.R.Rep.No. 99-612 at 12 (1986). The phrase as used in the credit card fraud statute means that the offender is conscious of the natural consequences of his action (i.e. that it is likely that someone will be defrauded) and intends that those consequences should occur (i.e., he intends that someone should be defrauded).[99]

The phrase "thereby furthers a fraud" insures that prosecutions are limited to cases where use of a computer is central to a criminal scheme rather those where a computer is used simply as a record-keeping convenience.[100]

Similarly, the demand that the value of converted property exceed $5,000 avoids the possibility that mere computer trespassing would be prosecuted as fraud under the theory that lost computer time could satisfy the "thing of value" element that

---

[99] H.R.Rep.No. 98-894 at 16-7 (1984)("A knowing state of mind with respect to an element of the offense is (1) an awareness of the nature of one' conduct, and (2) an awareness of or a firm belief in the existence of a relevant circumstance such as whether an access device was counterfeit before it was used or trafficked in. The Committee intends that the knowing state of mind requirement may be satisfied by proof that the actor was aware of a high probability of the existence of the circumstances, although a defense should succeed if it is proven that the actor actually believed that the circumstance did not exist after taking reasonable steps to warrant such belief. . . . The Committee intends that the term 'with the intent' have the same culpable state of mind as the term 'purpose' as used in the proposed Model Penal Code (§2.02). The distinction from a knowing state of mind was recently restated by Justice Rehnquist, '. . . a person who causes a particular result is said to act purposefully if he consciously desires that result, whatever the likelihood of that result happening from his conduct, while he is aid to act knowingly if he is aware that result is practically certain to follow from his conduct, whatever his desire may be as to that result.' *United States v. Bailey*, 444 U.S. 394, 404 (1980)").

[100] S.Rep.No. 99-432 at 9 (1986)("The Committee was concerned 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. If it were so patterned, the subsection might be construed as covering an individual who had devised a scheme or artifice to defraud solely because used a computer to keep records or to add up his potential 'take' from the crime. The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud. While such a tenuous link might be covered under current law where the instrumentality used is the mails or the wires, the Committee does not consider that link sufficient with respect to computers. To be prosecuted under this subsection, the use of the computer must be more directly linked to the intended fraud. That is, it must be used by the offender without authorization or in excess of his authorization to obtain property of another, which property furthers in the intended fraud").

separates the two offenses. The $5,000 threshold overcomes this problem while permitting prosecution for repeated intrusions, S.Rep.No. 104-357 at 9 (1996).

The case law available thus far confirms that the difficulty of maintaining a prosecution against even a repeated trespasser under paragraph 1030(a)(4). As *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), demonstrates. *Czubinski* involved an Internal Revenue Service employee who conducted a number of unauthorized searches of taxpayer files in an IRS computer system. The Court of Appeals overturned his conviction on four counts of violating paragraph 1030(a)(4) because it felt the government had failed to prove that the government had been defrauded, i.e, deprived of anything of value.[101]

Penalties.

Violations are punishable by imprisonment for not more than 5 years (not more than 10 years for subsequent offenses) and/or a fine of not more than $250,000 (not more than $500,000 for organizations), 18 U.S.C. 1030(c)(4); 18 U.S.C. 3571.[102] The same sentencing guideline, U.S.S.G. §2B1.1, covers both fraud under paragraph 1030(a)(4), and damage under paragraph 1030(a)(5), although the escalators based on the amount of loss inflicted are likely to be more telling in the case of wide-spread damage caused by the release of a worm or virus. As discussed earlier, violations of any paragraph of subsection 1030(a) may lead to the confiscation of the fruits of the offense and to orders to make restitution to the victims of the offense. Victims may sue for compensatory damages and/or injunctive relief under subsection 1030(g).[103]

---

[101] "The 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 sued 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. [The district court, in denying a motion to dismiss the computer fraud counts in the indictment, found that the indictment sufficiently alleged that the confidential taxpayer information was itself a thing of value to Czubinski, given his ends. The indictment, or course, alleged specific uses for the information, such as creating dossiers on KKK members, that were not proven at trial]," *United States v. Czubinski*, 106 F.3d at 1078 (portions of footnote 15 of the Court's opinion in brackets). See also, *United States v. DeMonte*, 25 F.3d 343 (6th Cir. 1994)(authority of sentencing court to order probation instead of imprisonment pursuant to a downward departure, on the basis of extraordinary circumstances, from the applicable sentencing guidelines for a violation of 18 U.S.C. 1030(4) that occurred when the defendant, a Veterans' Administration supervisory accountant made fraudulent entries in a VA computer system that result in payments to a fictitious company).

[102] The governing Sentencing Guideline calculates the applicable sentencing ranges below the statutory 5 and 10 year maximum penalties based on the amount of loss and the number of victims related to the offense, U.S.S.G. §2B1.1.

[103] Civil plaintiffs utilizing 1030(g) tend to have been more likely to successfully litigate under a violation of 1030(a)(4) than in the criminal context. See e.g. *Creative Computing*

Other Crimes.

Paragraph 1030(a)(4) prohibits unauthorized use of a government computer, a bank computer or a computer used in interstate or foreign commerce as an integral part of a fraud. Its companions at federal criminal law include general criminal statutes, statutes proscribing theft or fraud of federal property, those that outlaw the theft or fraud of the property of financial institutions, and those that prohibit theft or fraud involving property with an interstate or foreign commerce nexus.

Interstate & foreign commerce.

Interstate or foreign transportation of stolen property. Whether a hacker, who steals information stored in a computer, violates any of the general federal theft statutes depends upon whether the particular statute covers intangible property, and if not, whether the victim has been defrauded of intangible in addition to tangible property. For instance, the Supreme Court has noted that 18 U.S.C. 2314, that outlaws the interstate transportation of stolen goods, wares, or merchandise,[104] "contemplate[s] a physical identity between the items unlawfully obtained and those eventually transported."[105] Thus, the theft of information stored in a computer may be prosecuted under section 2314 only if the government can establish that it was accomplished in conjunction with the theft and transportation of a physical item, i.e., downloading information onto a stolen computer disk and then transporting the disk across a state line is covered, yet downloading information onto a computer disk that is transported but not stolen is not covered; however, courts have begun to differ in

---

v. Getloaded.com, 386 F.3d 930 (9th Cir. 2004)(court found that plaintiff successfully demonstrated loss of business as economic damages, and that the evidence supported a damage award and injunctive relief).

[104] "Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud; or

"Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, or induces any person or persons to travel in, or to be transported in interstate or foreign commerce in the execution or concealment of a scheme or artifice to defraud that person or those persons of money or property having a value of $5,000 or more; or

"Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any falsely made, forged, altered, or counterfeited securities or tax stamps, knowing the same to have been falsely made, forged, altered, or counterfeited; or

"Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any traveler's check bearing a forged countersignature; or

"Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce, any tool, implement, or thing used or fitted to be used in falsely making, forging, altering, or counterfeiting any security or tax stamps, or any part thereof –-

"Shall be fined under this title or imprisoned not more than ten years, or both. . . ." 18 U.S.C. 2314.

[105] *Dowling v. United States*, 473 U.S. 207, 216 (1985). *Dowling* involved the transportation of bootleg phonograph records which were not themselves stolen.

this interpretation and some have found an electronic file to be a tangible good within the meaning of section 2314.[106]

The federal statute proscribing theft from interstate carriers, 18 U.S.C. 659, speaks in terms of stealing "goods and chattels" under a variety of circumstances.[107] And it is presumably subject to the same analysis: section 659 applies only to the

---

[106] *United States v. Brown*, 925 F.2d 1301, 1305-309 (10th Cir. 1991); *United States v. Lyons*, 992 F.2d 1029, 1033 (10th Cir. 1993)("In *Brown*, we applied the Supreme Court's decision in *Dowling v. United States*, 474 U.S. 207 (1985) to computer software, and held that the intangible intellectual property of a computer program standing alone cannot constitute goods, wares or merchandise within the meaning of 18 U.S.C. 2314. The fact that Mr. Lyons stole the software in conjunction with the theft of tangible hardware distinguishes this case from *Brown. Brown* recognizes that the theft of intangible intellectual property in conjunction with the theft of tangible property falls within the ambit of §2314. Unlike the present case, there was no evidence in *Brown* that [the] defendant was involved in the physical theft or transportation of stolen tangible property"); *United States v. Martin*, 228 F.3d 1, 14 (1st Cir. 2000)(section 2314 applies "when there has been some tangible item taken, however insignificant or valueless it may be, absent the intangible component"). But see *United States v. Riggs*, 739 F. Supp 414, 420 (N.D. Ill. 1990) which found the electronic transfer of proprietary information to be covered by this statute ("if the information in [the plaintiff's] text file had been affixed to a floppy disk, or printed out on a computer printer, then [defendant's] transfer of that information across state lines would clearly constitute the transfer of goods, wares, or merchandise within the meaning of § 2314. This court sees no reason to hold differently simply because [defendant] stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferrable, accessible, even salable form."). See also *United States v. Farraj*, 142 F. Supp. 2d 484 (S.D.N.Y. 2001)(court disagreeing with *Brown* and the 10th Circuit line of cases, and instead determined "the view most closely analogous to Second Circuit doctrine is that which holds that the transfer of electronic documents via the internet across state lines does fall within the purview of § 2314.").

If section 2314 does apply to a given case, then section 2315 that prohibits receipt of stolen property may also be implicated.

[107] "Whoever embezzles, steals, or unlawfully takes, carries away, or conceals, or by fraud or deception obtains from any pipeline system, railroad car . . . with intent to convert to his own use any goods or chattels moving as or which are a part of or which constitute an interstate or foreign shipment of freight, express, or other property; or

"Whoever buys or receives or has in his possession any such goods or chattels, knowing the same to have been embezzled or stolen; or

"Whoever embezzles, steals, or unlawfully takes, carries away, or by fraud or deception obtains with intent to convert to his own use any baggage which shall have come into the possession of any common carrier for transportation in interstate or foreign commerce . . .

or

"Whoever embezzles, steals, or unlawfully takes by any fraudulent device, scheme, or game, from any railroad car, bus, vehicle, steamboat, vessel, or aircraft operated by any common carrier moving in interstate or foreign commerce or from any passenger thereon any money, baggage, goods, or chattels . . . .

"Shall in each case be fined under this title or imprisoned not more than ten years, or both; but if the amount or value of such money, baggage, goods or chattels does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both. . . ." 18 U.S.C. 659.

theft of physical items; even if all of the other elements are satisfied, computer fraud is proscribed by section 659 only where in involves the theft of physical item.

Wire fraud. Although the wire fraud statute, 18 U.S.C. 1343, does not refer to "things of value," a phrase that encompass both the tangible and the intangible, neither does it refer exclusively to physical items such as "goods, wares, merchandises, securities or money." Rather it condemns the use of interstate or foreign wire communications pursuant to a scheme to defraud another of "money or property."[108] The Supreme Court has made it clear that "property" within its purview may include confidential information,[109] and various federal courts have made it clear that confidential information in computer storage is no less favored.[110] In fact, one commentator claims that "[t]he wire fraud statute, 18 U.S.C. 1343, has produced more convictions for computer-related crimes than §1030 or any other computer-specific statute."[111]

Economic espionage. The Economic Espionage Act, among other things, outlaws computerized burglary committed in a commercial setting, 18 U.S.C. 1832.[112] It makes it a federal crime to steal certain trade secrets, or to receive such

---

[108] "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both," 18 U.S.C. 1343; see generally, *Nineteenth Survey of White Collar Crime: Mail and Wire Fraud*, 41 AMERICAN CRIMINAL LAW REVIEW 865 (2004); *Criminal and Civil RICO: Traditional Canons of Statutory Interpretation and the Liberal Construction Clause*, 30 COLUMBIA JOURNAL OF LAW & SOCIAL PROBLEMS 41 (1996); Lynch, *RICO: The Crime of Being a Criminal*, 87 COLUMBIA LAW REVIEW 661 (Pts. I & II), 920 (Pts. III & IV) (1987).

[109] *Carpenter v. United States*, 484 U.S. 19, 26 (1987).

[110] *United States v. Martin*, 228 F.3d 1, 16 (1st Cir. 2000); *United States v. Czubinski*, 106 F.3d 1069, 1073-76 (1st Cir. 1997); *United States v. Wang*, 898 F.Supp. 758, 760 (D.Colo. 1995); *United States v. Seidlitz*, 589 F.2d 152, 160 (4th Cir. 1978).

[111] Olivenbaum, *<CTRL><ALT><DELETE>: Rethinking Federal Computer Crime Legislation*, SETON HALL LAW REVIEW 574, 625 (1997).

[112] "(a) Whoever, with intent to convert a trade secret,*, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly –

"(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

"(2) without authorization copies, duplicates, sketches, draws photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

"(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

"(4) attempts to commit any offense described in paragraphs (1) through (3); or

trade secrets with the knowledge they have been stolen, or to conspire or attempt to steal them, or to conspire or attempt to receive them knowing they have been stolen. To be covered by the protective umbrella of section 1832, information must (1) have a nexus interstate or foreign commerce; (2) be a secret; and (3) have some trade value.

Information meets the commerce nexus when it is associated with a product that is marketed across state lines, i.e., if it is "related to or included in a product that is produced for or placed in interstate or foreign commerce," 18 U.S.C. 1832(a). Information is considered "secret" if it is "not generally known to the public or to the business, scientific, or education community in which [its] owner might seek to use the information" and its owner takes reasonable steps to maintain its confidentiality, H.R.Rep.No. 788 at 12; 18 U.S.C. 1839(3).

But what makes section 1832 a particularly effective shield against computerized burglary in a commercial setting is that the trade secret information it protects includes "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing," 18 U.S.C. 1839(3).

Violations of section 1832 are punishable by imprisonment for not more than 10 years and/or a fine of not more than the greater of twice the amount of pecuniary gain or loss resulting from the offense or $250,000 (not more than $5 million if the offender is an organization).

"(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, – shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

"(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000," 18 U.S.C. 1832.

* "'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if – (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public," 18 U.S.C. 1839(3); see generally, *Nineteenth Survey of White Collar Crime, Intellectual Property Crimes*, 41 AMERICAN CRIMINAL LAW REVIEW 809 (2004); Pooley, Lemley & Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEXAS INTELLECTUAL PROPERTY LAW JOURNAL 177 (1997).

Credit card fraud. Section 1029 of title 18 (credit card fraud) and section 1030 (computer fraud) share a common recent history.[113] Like section 1030, section 1029 has undergone rather regular fine-tuning since its initial passage in 1984 as part of the Comprehensive Crime Control Act of that year.[114] Unlike section 1030, it has a single, uniformly applicable jurisdictional base: it applies to offenses that "affect interstate or foreign commerce."[115]

The two overlap where section 1029 outlaws the deception of commercial computer systems through the improper use of an "access device" to acquire cash, credit, merchandise, or services.[116]

An access device is (1) any –

- card
- plate
- code
- personal identification number
- electronic serial number
- mobile identification number, or

---

[113] Each was enacted in part due to concerns about the breadth of a more narrowly crafted ancestor whose prohibitions continue in effect. In the case of section 1029, there were questions whether 15 U.S.C. 1644 (Truth in Lending Act) that outlaws the fraudulent use of credit cards could reach counterfeiting or the use of stolen credit card account numbers, H.R.Rep.No. 894, 98th Cong., 2d Sess. 5 (1984). In the case of section 1030, similar questions were raised about sweep of 15 U.S.C. 1693n (Electronic Funds Transfer Act) that outlaws the fraudulent use of bank debit cards), Id. See generally, *What Constitutes Violation of 18 USCS §1029, Prohibiting Fraud or Related Activity in Connection with Credit Card or Other Credit Access Device*, 115 ALR FED 213 (2005).

[114] Pub.L.No. 98-473, 98 Stat. 2183, 2190 (1984). Section 1029 was amended by Pub.L.No. 99-646, 100 Stat. 3601 (1986); Pub.L.No. 101-647, 104 Stat. 4831 (1990); Pub.L.No. 103-322, 108 Stat. 2087, 2148 (1994); Pub.L.No. 103-414, 108 Stat. 4291 (1994); Pub.L. No. 104-294, 110 Stat. 3501 (1996); Pub.L.No. 105-172, 112 Stat. 53 (1998); Pub.L. No. 107-25,115 Stat. 342 (2001); Pub.L.No. 107-273, 116 Stat. 1808 (2002).

[115] Recent cases suggest that the interstate nexus must be clearly identifiable but have yet to identify the point, if any, at which the connection becomes too tenuous to support a claim of an affect on interstate commerce, see e.g., *United States v. Bolton*, 68 F.3d 396, 400 n.3 (10th Cir. 1995)(large majority of stolen credit cards in the defendant's possession had out of state addresses printed on them); *United States v. Clayton*, 108 F.3d 1114, 1118 (9th Cir. 1997). Since the misconduct proscribed is commercial in nature the question is not one of Congressional power but whether in a given case the government can and has proven that the particular misconduct "affects interstate or foreign commerce," compare *United States v. Morrison*, 529 U.S. 598, 608-9 (2000) and *United States v. Lopez*, 514 U.S. 549, 558-59 (1995)(Congress may regulate the instrumentalities and use of the channels of interstate commerce and activities that have a substantial relation to interstate commerce), with, *Jones v. United States*, 529 U.S. 848, 852 (2000) (a statute that outlaws the destruction of property "used" in commerce does not protect residential property not shown to have been used for any commercial purpose) and *Gonzales v. Raich*, 125 S. Ct. 2195, 2205 (2005) (federal government could regulate "an economic class" of intrastate activities–even if the activity itself, is noncommercial–if they are rationally related to or substantially effecting interstate commerce).

[116] As discussed below section 1029 also overlaps paragraph 1030(a)(6) that relates to trafficking in a particular access device, computer passwords.

• any account number or other telecommunications service, equipment, or instrument identifier, or other means of account access;

(2) that either
(a) can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or
(b) can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument), 18 U.S.C. 1029(e)(1).

The level of intent for each of the several crimes established in section 1029 is the same as that often used for section 1030 – "knowing and with the intent to defraud." Thus, criminal liability under section 1029 requires that the offender know that his or her actions are likely to deprive another of something of value and demands that the offender means for that deprivation to occur.[117]

Section 1029 establishes three types of crimes: misuse of access devices, conduct in anticipation of misuse of access devices, and attempts or conspiracies to commit one of these substantive violations. The misuse crimes include:

- use of a *counterfeit* access device;[118] a counterfeit access device is one that is "counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device" (§1029(e)(2)(emphasis added));[119]

- use of a *unauthorized* access device resulting in a loss or gain over the course of 1 year worth than $1,000;[120] an unauthorized access

---

[117] "'With intent to defraud' means that the offender has a conscious objective, desire or purpose to deceive another person, and to induce such other person, in reliance upon such deception, to assume, create, transfer, alter or terminate a right, obligation, or power with reference to property," S.Rep.No. 368 at 7.

[118] "Whoever – (1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(1).

[119] "The term 'fictitious' is intended to cover a number of different types of counterfeit devices, including representations, depictions or facsimiles of an access device. The definition is intended to be sufficiently broad to cover components of an access device or a counterfeit access device, but would exclude indistinguishable raw materials. The components would include elements of devices that are legitimate but obtained or used with an intent to defraud. Thus, any identifiable component, whether it is in fact an actual component that has been obtained in some fashion by a perpetrator with an intent to defraud or a false or counterfeit substitute for a legitimate component, would fall within the definition of counterfeit access device. The committee intends the term 'component' to include incomplete access devices or counterfeit access devices, such as any mag strips, holograms, signature panels, microchips, and blank cards of so-called 'white plastic.'" H.R.Rep.No. 98-894 at 19 (1984).

[120] "Whoever . . . knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this

device is one that has been "lost, stolen, expired, revoked, canceled, or obtained with intent to defraud" (§1029(e)(3)(emphasis added)); and

- use of an access device "issued to another person" resulting in a loss or gain over the course of 1 year worth than $1,000; again each of the uses is only criminal if done knowingly and with an intent to defraud;[121]

The "preparation" offenses of section 1029 each extend only to misconduct that affects interstate or foreign commerce and only to misconduct committed knowingly and with an intent to defraud, 18 U.S.C. 1029(a). They include:

- possession of 15 or more counterfeit or unauthorized access devices;[122]

- possession of "device-making" equipment (§1029(a)(4);[123] essentially counterfeiting paraphernalia;[124]

- offering another an access device or offering to sell information concerning an access device, without the authorization of the issue of the device;[125]

---

section," 18 U.S.C. 1029(a)(2).

[121] "Whoever . . . knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000 . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(5).

[122] "Whoever . . . knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(3).

[123] "Whoever . . . knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(4).

[124] "As used in this section . . . the term 'device-making equipment' means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device," 18 U.S.C. 1029(e)(6).

[125] "Whoever . . . without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -- (A) offering an access device; or (B) selling information regarding or an application to obtain an access device . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(6).

- use of a telecommunications device modified or altered to permit the unauthorized receipt of telecommunications services;[126]

- use of a scanner;[127] i.e., illegal wiretapping or electronic eavesdropping equipment;[128]

- possession of computer equipment used to avoid telecommunications charges, i.e., possession of "hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services;"[129] and

- causing another to present credit card slips for payment with the intent to defraud.[130]

Paragraph 1029(b)(1) makes it a separate offense to attempt to commit any of the substantive crimes in subsection 1029(a) just described.[131] Paragraph 1029(b)(2)

---

[126] "Whoever . . . knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(7).

[127] "Whoever . . . knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(8).

[128] "The term 'scanning receiver' means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument," 18 U.S.C. 1029(e)(8).

[129] "Whoever . . . knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that the instrument may be used to obtain telecommunications service without authorization . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(9).

[130] "Whoever . . . without the authorization of the credit card system member* or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(10).

* "As used in this section . . . [t]he term 'credit card system member' means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system," 18 U.S.C. 1029(e)(7).

[131] "Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(b)(1).

makes it a separate offense to conspire to commit any of them.[132] Attempt to carries the same penalties as the completed offense (imprisonment either for not more than 10 or not more than 15 years), but conspiracy is punishable by imprisonment for not more than half the maximum terms applicable to the underlying offense (imprisonment for not more than 5 or not more than 7.5 years), 18 U.S.C. 1029(b). One reason for the distinction may be that while attempt is merged in the completed offense so that an offender may be punished for either but not both, the crime of conspiracy is ordinarily not merged in the substantive offense so that punishment for either or both is permitted.

In any event, the maximum penalties are determined by those set for the underlying violations of subsection 1029: (1) imprisonment for not more than 10 years for first time offenses involving:

- use of counterfeit access devices, 18 U.S.C. 1029(a)(1);
- use of unauthorized access devices, 18 U.S.C. 1029(a)(2);
- possession of 15 or more counterfeit or unauthorized access devices, 18 U.S.C. 1029(a)(3);
- unauthorized sale of an access device, 18 U.S.C. 1029(a)(6);
- possession of a device designed to avoid telephone charges, 18 U.S.C. 1029(a)(7); or
- fraudulently causing another to present credit car slips for payment, 18 U.S.C. 1029(a)(10);
- and imprisonment for not more than 15 years for first time offenses involving:
- possession of counterfeiting equipment, 18 U.S.C. 1029(a)(4);
- use of another's access device to defraud, 18 U.S.C. 1029(a)(5);
- possession of a scanner, 18 U.S.C. 1029(a)(8); or
- possession of equipment designed to avoid communications service charges, 18 U.S.C. 1029(a)(9).[133]

---

[132] "Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both," 18 U.S.C. 1029(b)(2).

[133] Offenders are subject to fines and forfeiture as well, "(1) . . .The punishment for an offense under subsection (a) of this section is – (A) in the case of an offense that does not occur after a conviction for another offense under this section – "(i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and (ii) if the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

"(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

"(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

"(2) Forfeiture procedure.–The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial

Defrauding the federal government.

Conspiracy. The same statute that makes it a crime to conspire to violate federal law also makes it a federal crime to conspire to defraud the United States, 18 U.S.C. 371.[134] Unlike the mail and wire fraud statutes, a successful prosecution for conspiracy to defraud the United States does not require a showing that the defendant sought to deprive the United States or anyone else of money or property.[135] This lesser known branch of the statute has extraordinary range and "reaches any conspiracy for the purpose of impairing, obstructing or defeating the lawful function of any department of the Government."[136] There need be no evidence of any other underlying substantive offense or purpose.[137] "The government need only show (1) that the defendant entered into an agreement (2) to obstruct a lawful function of the government (3) by deceitful or dishonest means and (4) at least one overt act in furtherance of the conspiracy."[138]

Theft of federal government information. Prosecuting computer fraud under a statute that outlaws the interstate transportation of stolen "goods, wares, merchandise, securities or money" may be an awkward fit. The general theft of government property statute, 18 U.S.C. 641, seems a better match, however, for that provision outlaws the misappropriation of any "thing of value" belonging to or in the

---

proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section," 18 U.S.C. 1029(c).

[134] "If two or more persons conspire . . . to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both," 18 U.S.C. 371.

[135] *United States v. Goldberg*, 105 F.3d 770, 773 (1st Cir. 1997); *United States v. Clark*, 139 F.3d 485, 488-89 (5th Cir. 1998); *United States v. Gosselin World Wide Moving*,__F.3d__, 2005 WL 1389531, at *11 (4th Cir. June 14, 2005).

[136] *Tanner v. United States*, 483 U.S. 107, 128 (1987), citing, *Dennis v. United States*, 384 U.S. 855, 861 (1966); *Hass v. Henkel*, 216 U.S. 462, 479 (1910); *Glasser v. United States*, 315 U.S. 60, 66 (1942); *Hammerschmidt v. United States*, 265 U.S. 182, 188 (1924); *Gosselin World Wide Moving*, __F.3__, 2005 WL 1389531, at *11.

[137] *United States v. Ballistrea*, 101 F.3d 827, 832 (2d Cir. 1996)("so long as deceitful or dishonest means are employed to obstruct governmental functions, the impairment need not involve the violation of a separate statute"); *United States v. Khalife*, 106 F.3d 1300, 1303 (6th Cir. 1997); *United States v. Douglas*, 398 F.3d 407, 412 (6th Cir. 2005)("a conviction under section 371 does not require the government to prove a violation of a separate substantive statute").

[138] *United States v. Ballistrea*, 101 F.3d at 832; *United States v. Dean*, 55 F.3d 640, 647 (D.C.Cir. 1994); *United States v. Hansen*, 262 F.3d 1217, 1246 (11th Cir. 2001)("To obtain a conviction under 18 U.S.C. § 371, the government must show: (1) the existence of an agreement to achieve an unlawful objective; (2) the defendant's knowing and voluntary participation in the conspiracy; and (3) the commission of an overt act in furtherance of the conspiracy.").

possession of the federal government.[139] The courts have applied section 641 to the misappropriation of property that lacks any necessary corporal features.[140]

Theft or fraud involving government computers. There are also a host of federal criminal statutes that proscribe fraud in one form or other, more than a few of which would cover the unauthorized manipulation of federal computers as an integral part of a scheme to defraud. Two of the more prominent, the false statement statute, 18 U.S.C. 1001 (false statements on a matter within the jurisdiction of a federal agency or department) and conspiracy to defraud the United States, 18 U.S.C. 371, have already been mentioned. Others include 18 U.S.C. 1031 (major procurement fraud against the United States);[141] 18 U.S.C. 1035 (false statements relating to health care);[142] 18 U.S.C. 1014 (false statements on federally insured loan

---

[139] "Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

"Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted –

"Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property in the aggregate, combining amounts from all the counts for which the defendant is convicted in a single case, does not exceed the sum of $1,000, he shall be fined under this title or imprisoned not more than one year, or both."

"The word 'value' means face, par, or market value, or cost price, either wholesale or retail, whichever is greater," 18 U.S.C. 641.

[140] See e.g., *United States v. Forman*, 180 F.3d 766, 767-68 (6th Cir. 1999)(information from a confidential government report concerning a criminal investigation); *United States v. Collins*, 56 F.3d 1416, 1419-420 (D.C.Cir. 1995)(computer time and storage); *United States v. Martzkin*, 14 F.3d 1014, 1018-21 (4th Cir. 1994)(bids on government contracts); *United States v. Jeter*, 775 F.2d 670, 680 (6th Cir. 1985)(information as to matters occurring before a federal grand jury); *United States v. Girard*, 601 F.2d 69, 70-1 (2d Cir. 1979) (identity of government undercover agents); *United States v. Lambert*, 446 F.Supp. 890, 892-95 (D.Conn. 1978)(information stolen from a DEA computer data base).

[141] "(a) Whoever knowingly executes, or attempts to execute, any scheme or artifice with the intent – (1) to defraud the United States; or (2) to obtain money or property by means of false or fraudulent pretenses, representations, or promises – in any procurement of property or services as a prime contractor with the United States or as a subcontractor or supplier on a contract in which there is a prime contract with the United States, if the value of the contract, subcontract, or any constituent part thereof, for such property or services is $1,000,000 or more shall, subject to the applicability of subsection (c) of this section, be fined not more than $1,000,000, or imprisoned not more than 10 years, or both.

"(b) The fine imposed for an offense under this section may exceed the maximum otherwise provided by law, if such fine does not exceed $5,000,000 and – (1) the gross loss to the Government or the gross gain to a defendant is $500,000 or greater; or (2) the offense involves a conscious or reckless risk of serious personal injury.

"(c) The maximum fine imposed upon a defendant for a prosecution including a prosecution with multiple counts under this section shall not exceed $10,000,000. . . ." 18 U.S.C. 1031.

[142] "Whoever, in any matter involving a health care benefit program, knowingly and willfully – (1) falsifies, conceals, or covers up by any trick, scheme, or device a material

and credit applications);[143] 18 U.S.C. 1010, 1012 (false statements concerning

fact; or (2) makes any materially false, fictitious, or fraudulent statements or representations, or makes or uses any materially false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry, in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 5 years, or both," 18 U.S.C. 1035(a).

[143] "Whoever knowingly makes any false statement or report, or willfully overvalues any land, property or security, for the purpose of influencing in any way the action of the Farm Credit Administration, Federal Crop Insurance Corporation or a company the Corporation reinsures, the Secretary of Agriculture acting through the Farmers Home Administration or successor agency, the Rural Development Administration or successor agency, any Farm Credit Bank, production credit association, agricultural credit association, bank for cooperatives, or any division, officer, or employee thereof, or of any regional agricultural credit corporation established pursuant to law, or a Federal land bank, a Federal land bank association, a Federal Reserve bank, a small business investment company, as defined in section 103 of the Small Business Investment Act of 1958 (15 U.S.C. 662), or the Small Business Administration in connection with any provisions of that Act, a Federal credit union, an insured State-chartered credit union, any institution the accounts of which are insured by the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, any Federal home loan bank, the Federal Housing Finance Board, the Federal Deposit Insurance Corporation, the Resolution Trust Corporation, the Farm Credit System Insurance Corporation, or the National Credit Union Administration Board, a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978), or an organization operating under section 25 or section 25(a) of the Federal Reserve Act, upon any application, advance, discount, purchase, purchase agreement, repurchase agreement, commitment, or loan, or any change or extension of any of the same, by renewal, deferment of action or otherwise, or the acceptance, release, or substitution of security therefor, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both. . . ." 18 U.S.C. 1014.

various HUD transactions);[144] and 18 U.S.C. 287 (false claims against the United States).[145]

Bank fraud. Although less numerous, several federal criminal laws outlaw defrauding financial institutions in language similar to the prohibitions against defrauding the United States: e.g., 18 U.S.C. 1344 (bank fraud);[146] 18 U.S.C. 656 (theft or embezzlement by bank officers or employees);[147] 18 U.S.C. 657 (theft or

---

[144] "Whoever, for the purpose of obtaining any loan or advance of credit from any person, partnership, association, or corporation with the intent that such loan or advance of credit shall be offered to or accepted by the Department of Housing and Urban Development for insurance, or for the purpose of obtaining any extension or renewal of any loan, advance of credit, or mortgage insured by such Department, or the acceptance, release, or substitution of any security on such a loan, advance of credit, or for the purpose of influencing in any way the action of such Department, makes, passes, utters, or publishes any statement, knowing the same to be false, or alters, forges, or counterfeits any instrument, paper, or document, or utters, publishes, or passes as true any instrument, paper, or document, knowing it to have been altered, forged, or counterfeited, or willfully overvalues any security, asset, or income, shall be fined under this title or imprisoned not more than two years, or both," 18 U.S.C. 1010.

"Whoever, with intent to defraud, makes any false entry in any book of the Department of Housing and Urban Development or makes any false report or statement to or for such Department; or whoever receives any compensation, rebate, or reward, with intent to defraud such Department or with intent unlawfully to defeat its purposes; or whoever induces or influences such Department to purchase or acquire any property or to enter into any contract and willfully fails to disclose any interest which he has in such property or in the property to which such contract relates, or any special benefit which he expects to receive as a result of such contract – shall be fined under this title or imprisoned not more than one year, or both," 18 U.S.C. 1012.

[145] "Whoever makes or presents to any person or officer in the civil, military, or naval service of the United States, or to any department or agency thereof, any claim upon or against the United States, or any department or agency thereof, knowing such claim to be false, fictitious, or fraudulent, shall be imprisoned not more than five years and shall be subject to a fine in the amount provided in this title," 18 U.S.C. 287; see generally, *Nineteenth Survey of White Collar Crime: False Claims*, 41 AMERICAN CRIMINAL LAW REVIEW 527 (2004).

[146] "Whoever knowingly executes, or attempts to execute, a scheme or artifice – (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises – shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both," 18 U.S.C. 1344; see generally, *Nineteenth Survey of White Collar Crime: Financial Institutions Fraud*, 41 AMERICAN CRIMINAL LAW REVIEW 671 (2004).

[147] "Whoever, being an officer, director, agent or employee of, or connected in any capacity with any Federal Reserve bank, member bank, depository institution holding company, national bank, insured bank, branch or agency of a foreign bank, or organization operating under section 25 or section 25(a) of the Federal Reserve Act, or a receiver of a national bank, insured bank, branch, agency, or organization or any agent or employee of the receiver, or a Federal Reserve Agent, or an agent or employee of a Federal Reserve Agent or of the Board of Governors of the Federal Reserve System, embezzles, abstracts, purloins or willfully misapplies any of the moneys, funds or credits of such bank, branch, agency, or

embezzlement by officer or employee of lending, credit and insurance institutions);[148] 18 U.S.C. 1005 (false entries bank officers or employees);[149] 18 U.S.C. 1006 (false

---

organization or holding company or any moneys, funds, assets or securities intrusted to the custody or care of such bank, branch, agency, or organization, or holding company or to the custody or care of any such agent, officer, director, employee or receiver, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both: but if the amount embezzled, abstracted, purloined or misapplied does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both. . . ." 18 U.S.C. 656.

[148] "Whoever, being an officer, agent or employee of or connected in any capacity with the Federal Deposit Insurance Corporation, National Credit Union Administration, Office of Thrift Supervision, the Resolution Trust Corporation, any Federal home loan bank, the Federal Housing Finance Board, Farm Credit Administration, Department of Housing and Urban Development, Federal Crop Insurance Corporation, the Secretary of Agriculture acting through the Farmers Home Administration or successor agency, the Rural Development Administration or successor agency or the Farm Credit System Insurance Corporation, a Farm Credit Bank, a bank for cooperatives or any lending, mortgage, insurance, credit or savings and loan corporation or association authorized or acting under the laws of the United States or any institution, other than an insured bank (as defined in section 656), the accounts of which are insured by the Federal Deposit Insurance Corporation or by the National Credit Union Administration Board or any small business investment company, or any community development financial institution receiving financial assistance under the Riegle Community Development and Regulatory Improvement Act of 1994, and whoever, being a receiver of any such institution, or agent or employee of the receiver, embezzles, abstracts, purloins or willfully misapplies any moneys, funds, credits, securities or other things of value belonging to such institution, or pledged or otherwise intrusted to its care, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both; but if the amount or value embezzled, abstracted, purloined or misapplied does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both," 18 U.S.C. 657.

[149] "Whoever, being an officer, director, agent or employee of any Federal Reserve bank, member bank, depository institution holding company, national bank, insured bank, branch or agency of a foreign bank, or organization operating under section 25 or section 25(a) of the Federal Reserve Act, without authority from the directors of such bank, branch, agency, or organization or company, issues or puts in circulation any notes of such bank, branch, agency, or organization or company; or whoever, without such authority, makes, draws, issues, puts forth, or assigns any certificate of deposit, draft, order, bill of exchange, acceptance, note, debenture, bond, or other obligation, or mortgage, judgment or decree; or whoever makes any false entry in any book, report, or statement of such bank, company, branch, agency, or organization with intent to injure or defraud such bank, company, branch, agency, or organization, or any other company, body politic or corporate, or any individual person, or to deceive any officer of such bank, company, branch, agency, or organization, or the Comptroller of the Currency, or the Federal Deposit Insurance Corporation, or any agent or examiner appointed to examine the affairs of such bank, company, branch, agency, or organization, or the Board of Governors of the Federal Reserve System; [or] whoever with intent to defraud the United States or any agency thereof, or any financial institution referred to in this section, participates or shares in or receives (directly or indirectly) any money, profit, property, or benefits through any transaction, loan, commission, contract, or any other act of any such financial institution – shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both. . . ." 18 U.S.C. 1005.

entries by officers or employees of federal credit institutions);[150] 18 U.S.C. 1007 (false statements to influence the Federal Deposit Insurance Corporation).[151]

General crimes.

CAN-SPAM Act of 2003. The criminal provisions of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 18 U.S.C. 1037, generally broadens the type of coverage given by section 1030[152] and specifically adds to the federal government's ability to prosecute hackers who use e-mail for fraudulent purposes.[153]

---

[150] "Whoever, being an officer, agent or employee of or connected in any capacity with the Federal Deposit Insurance Corporation, National Credit Union Administration, Office of Thrift Supervision, any Federal home loan bank, the Federal Housing Finance Board, the Resolution Trust Corporation, Farm Credit Administration, Department of Housing and Urban Development, Federal Crop Insurance Corporation, the Secretary of Agriculture acting through the Farmers Home Administration or successor agency, the Rural Development Administration or successor agency, or the Farm Credit System Insurance Corporation, a Farm Credit Bank, a bank for cooperatives or any lending, mortgage, insurance, credit or savings and loan corporation or association authorized or acting under the laws of the United States or any institution, other than an insured bank (as defined in section 656), the accounts of which are insured by the Federal Deposit Insurance Corporation, or by the National Credit Union Administration Board, or any small business investment company, with intent to defraud any such institution or any other company, body politic or corporate, or any individual, or to deceive any officer, auditor, examiner or agent of any such institution or of department or agency of the United States, makes any false entry in any book, report or statement of or to any such institution, or without being duly authorized, draws any order or bill of exchange, makes any acceptance, or issues, puts forth or assigns any note, debenture, bond or other obligation, or draft, bill of exchange, mortgage, judgment, or decree, or, with intent to defraud the United States or any agency thereof, or any corporation, institution, or association referred to in this section, participates or shares in or receives directly or indirectly any money, profit, property, or benefits through any transaction, loan, commission, contract, or any other act of any such corporation, institution, or association, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both," 18 U.S.C. 1006.

[151] "Whoever, for the purpose of influencing in any way the action of the Federal Deposit Insurance Corporation, knowingly makes or invites reliance on a false, forged, or counterfeit statement, document, or thing shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both," 18 U.S.C. 1007.

[152] 18 U.S.C. 1037(a)(1) provides that anyone who affects interstate commerce and knowingly "accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic messages from or through such computer...or conspires to do so, shall be punished as provided in subsection (b)." CAN-SPAM thus overlaps in some part the general trespassing in government cyberspace provisions found in 1030(a)(3). This statute also offers much broader protection to both private and government computers because it does not require that the hacker "obtained information" (1030(a)(1) &(2)), obtained anything of value (1030(a)(4)), or caused any damage (1030(a)(5)).

[153] "(a) In general.--Whoever, in or affecting interstate or foreign commerce, knowingly--(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such

Five different crimes are described by section 1037, and all include the elements of "affecting interstate or foreign commerce" as well as knowingly and intentionally doing the crimes, 18 U.S.C. 1037(a). The crimes include: (1) accessing a protected computer[154] and sending multiple[155] e-mail messages from that computer, 1037(a)(1); (2) using a protected computer to transmit commercial e-mails with the intent to "deceive or mislead recipients" about their origin, 1037(a)(2); (3) falsifying header information[156] and sending messages under the false information, 1037(a)(3); (4) registering for 5 or more e-mail accounts or two or more domain names using false identity information and sending multiple commercial e-mails therefrom, 1037(a)(4); falsely representing oneself to be the legitimate registrant of 5 or more Internet addresses and sending multiple commercial e-mails therefrom, 1037(a)(5).

Thus, a hacker who accesses a computer without authorization and generates spam, fraudulently falsifies an e-mail or e-mail account, or falsely represents himself to be the legitimate e-mail account owner can be prosecuted under CAN-SPAM.[157] The penalties include 5 years imprisonment if done in furtherance of a felony or if the defendant had previously been convicted of one of the crimes described in sections 1030 or 1037. 18 U.S.C. 1037(b)(1).[158] If the defendant violated (a)(1), or

---

computer, (2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages, (3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages, (4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or (5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b)." 18 U.S.C. 1037. For more information on CAN-SPAM, see Smith, *"Spam": An Overview of Issues Concerning Electronic Mail*, CRS. REP. No. RL 31953 (Mar. 23, 2005).

[154] CAN-SPAM defers to the definition given in 1030(e). 15 U.S.C. 7702(13).

[155] "Multiple" is defined as meaning more than 100 e-mail messages in one month or more than 1,000 in one year. 18 U.S.C. 1037 (d)(3).

[156] "Header Information" is defined as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message," 15 U.S.C. 7702(8).

[157] Because subsections (a)(2) through (a)(5) do not require the government to prove "unauthorized access", in any situations in which a hacker merely exceeds authorized access, or where this element is difficult to prove, if the defendant also sends misleading, fraudulent, multiple commercial e-mails then he is guilty of a felony.

[158] "(b) Penalties.– The punishment for an offense under subsection (a) is– (1) a fine under this title, imprisonment for not more than 5 years, or both, if– (A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or (B) the defendant has previously been convicted under this section or section 1030, or under the law

the victim experienced financial loss of more than $5,000, or the hacker obtained more than $5000, or the volume of e-mails sent or falsified registrations exceed a certain threshold, or the defendant is deemed the leader of a of a group of individuals violating the statute then the penalty increases to 3 years. 18 U.S.C. 1037(b)(2) "[I]n any other case" the penalty is 1 year imprisonment, 18 U.S.C. 1037(b)(3).[159] For all variations of the above described violations, the defendant is subject to a fine of no more than $250,000, 18 U.S.C. 3751; 18 U.S.C. 1037(b).

Copyright infringement. Computer software programs are ordinarily protected by copyright which generally precludes copying of the protected material except with the consent of the holder of the copyright. Willful copyright infringement for purposes of commercial advantage or private financial gain is a federal crime, 17 U.S.C. 506.

The copyright infringement provisions long imposed no impediment to those who denigrate the value of copyright protection by making protected material

---

of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system; (2) a fine under this title, imprisonment for not more than 3 years, or both, if– (A) the offense is an offense under subsection (a)(1); (B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations; (C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period; (D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period; (E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or (F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and (3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case."18 U.S.C. 1037(b).

[159] "(b) Penalties.– The punishment for an offense under subsection (a) is--(1) a fine under this title, imprisonment for not more than 5 years, or both, if--(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or (B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system; (2) a fine under this title, imprisonment for not more than 3 years, or both, if– (A) the offense is an offense under subsection (a)(1); (B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations; (C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period; (D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period; (E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or (F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and (3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case."18 U.S.C. 1037(b).

publicly available on the Internet as long as they do not so for purposes of commercial advantage or financial gain.[160] That is no longer the case. Congress has supplemented the financial component of the infringement prohibition with a proscription against infringement whose piracy involves more than $1000.[161] It also

---

[160] The Supreme Court has refused to allow the interstate stolen property statute, 18 U.S.C. 2314, to be used to supplement copyright law, *Dowling v. United States*, 473 U.S. 207 (1985). And at least one lower federal court has refused to allow the wire fraud statute, 18 U.S.C. 1343, to used to prosecute a electronic bulletin board operator who invited others to post copyright protected software to the bulletin board from which it might be download without charge thereby denying the copyright holders millions of dollars in royalties, *United States v. LaMacchia*, 871 F.Supp. 535 (D.Mass. 1994); see discussion in Heymann, *Legislating Computer Crime*, 34 HARVARD JOURNAL OF LEGISLATION 373 (1997).

[161] (1) In general.– Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed--(A) for purposes of commercial advantage or private financial gain; (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

(2) Evidence.– For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright.

(3) Definition.– In this subsection, the term "work being prepared for commercial distribution" means– (A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution–
(i) the copyright owner has a reasonable expectation of commercial distribution; and
(ii) the copies or phonorecords of the work have not been commercially distributed; or
(B) a motion picture, if, at the time of unauthorized distribution, the motion picture–
(i) has been made available for viewing in a motion picture exhibition facility; and
(ii) has not been made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a motion picture exhibition facility," 17 U.S.C. 506(a). See also *United States v. Rothberg*, 222 F. Supp. 2d 1009, 1018 (N.D. Ill. 2002)(stating that it "was partly a desire to plug the perceived LaMacchia gap that motivated Congress to pass the NET Act in December 1997").

Section 2319 provides an array of penalties: "(a) Any person who violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b), (c), and (d) and such penalties shall be in addition to any other provisions of title 17 or any other law.

"(b) Any person who commits an offense under section 506(a)(1)(A) of title 17– (1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500; (2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

"(c) Any person who commits an offense under section 506(a)(1)(B) of title 17– (1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or

added penalties for hacking into copyrighted material for profit or marketing the means to crack the encryption of copyrighted material.[162]

Attempt, conspiracy, and complicity. The same general observations concerning attempt, conspiracy and aiding and abetting noted for the simple trespass paragraph apply here. It is a separate crime to attempt to violate paragraph 1030(a)(4), 18 U.S.C. 1030(b). Those who attempt to do so or who aid and abet the violation of another are subject to the same penalties as those commit the substantive offense, 18 U.S.C. 1030(c), 2. The same is true of conspiracies except that

---

more; (2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.

"(d) Any person who commits an offense under section 506(a)(1)(C) of title 17– (1) shall be imprisoned not more than 3 years, fined under this title, or both; (2) shall be imprisoned not more than 5 years, fined under this title, or both, if the offense was committed for purposes of commercial advantage or private financial gain; (3) shall be imprisoned not more than 6 years, fined under this title, or both, if the offense is a second or subsequent offense; and (4) shall be imprisoned not more than 10 years, fined under this title, or both, if the offense is a second or subsequent offense under paragraph (2)," 18 U.S.C. 2319.

[162] "(a) . . . (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. . . .

"(b) . . . (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that-- (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof. (2) As used in this subsection – (A) to 'circumvent protection afforded by a technological measure' means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and (B) a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title. . . ." 17 U.S.C. 1201. This digital copyright law has also been used in tandem with section 1030(a)(2), in a civil case utilizing 1030(g). *Inquiry Management Systems v. Berkshire Information Systems*, 307 F. Supp. 2d 521 (S.D.N.Y. 2004)(court denied a motion to dismiss the 1030 action, and granted the dismissal of the copyright claims).

"Any person who violates section 1201 . . . willfully and for purposes of commercial advantage or private financial gain – (1) shall be fined not more than $500,000 or imprisoned for not more than 5 years, or both, for the first offense; and (2) shall be fined not more than $1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense," 17 U.S.C. 1204(a).

conspiracy to commit a felony carries a 5 year maximum of imprisonment, 18 U.S.C. 371.

*Money laundering.*Federal money laundering statutes outlaw depositing the proceedings from various illegal activities in financial institutions, 18 U.S.C. 1957, or plowing the proceedings back in the illicit venture, 18 U.S.C. 1956.[163] Directly or indirectly the predicate offenses ("specific unlawful activity") that will support a money laundering prosecution include section 1030 as well as several of the crimes that may also be implicated whenever paragraph 1030(a)(4) is violated: i.e., theft of government property (18 U.S.C. 641), credit card fraud (18 U.S.C. 1029), interstate transportation of stolen property (18 U.S.C. 2314), receipt of stolen property that has been transported in interstate or foreign commerce (18 U.S.C. 2315), and wire fraud (18 U.S.C. 1343).[164] The elements of the two crimes, 18 U.S.C. 1956 (promoting

---

[163] See generally, *Nineteenth Survey of White Collar Crime: Money Laundering*, 41 AMERICAN CRIMINAL LAW REVIEW 887 (2004); Gurulé, *The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity?*, 32 AMERICAN CRIMINAL LAW REVIEW 823 (1995).

[164] Section 641 is specifically listed as a money laundering predicate; sections 1029, 2314, 2315 and 1343 are RICO predicates and the money laundering definition adopts all the RICO predicates as its own. Section 1030 violations are not predicate themselves under either the money laundering statutes or RICO. The RICO predicates are listed *infra* in note 155; the full list of money laundering predicates includes:

"(A) any act or activity constituting an offense listed in section 1961(1) of this title except an act which is indictable under subchapter II of chapter 53 of title 31;

"(B) with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving– (i) the manufacture, importation, sale, or distribution of a controlled substance (as such term is defined for the purposes of the Controlled Substances Act); (ii) murder, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, or a crime of violence (as defined in section 16); (iii) fraud, or any scheme or attempt to defraud, by or against a foreign bank (as defined in paragraph 7 of section 1(b) of the International Banking Act of 1978)); (iv) bribery of a public official, or the misappropriation, theft, or embezzlement of public funds by or for the benefit of a public official; (v) smuggling or export control violations involving--(I) an item controlled on the United States Munitions List established under section 38 of the Arms Export Control Act (22 U.S.C. 2778); or (II) an item controlled under regulations under the Export Administration Regulations (15 C.F.R. Parts 730-774); or (vi) an offense with respect to which the United States would be obligated by a multilateral treaty, either to extradite the alleged offender or to submit the case for prosecution, if the offender were found within the territory of the United States;

"(C) any act or acts constituting a continuing criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848);

"(D) an offense under section 32 (relating to the destruction of aircraft), section 37 (relating to violence at international airports), 115 (influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member), 152 (concealment of assets; false oaths and claims; bribery), 175c (the variola virus), 215 (commissions or gifts for procuring loans), 351 (congressional or Cabinet officer assassination), any of sections 500 through 503 (certain counterfeiting offenses), 513 (securities of States and private entities), 541 (goods falsely classified), 542 (entry of goods by means of false statements), 545 (smuggling goods into the United States), 549 (removing goods from Customs custody), 641 (public money, property, or records), 656 (theft, embezzlement, or misapplication by

specific unlawful activity with the proceeds of unlawful activity) and 18 U.S.C. 1957 (engaging in monetary transactions derived from specified unlawful activity) are as follows. A violation of section 1956 occurs when:

- anyone, conducts or attempts to conduct a financial transaction
- knowingly using the proceeds derived from the theft of government property, or from wire fraud, or from theft or receipt of stolen property transported in interstate or foreign commerce,

---

bank officer or employee), 657 (lending, credit, and insurance institutions), 658 (property mortgaged or pledged to farm credit agencies), 666 (theft or bribery concerning programs receiving Federal funds), 793, 794, or 798 (espionage), 831 (prohibited transactions involving nuclear materials), 844(f) or (i) (destruction by explosives or fire of Government property or property affecting interstate or foreign commerce), 875 (interstate communications), 922(1) (the unlawful importation of firearms), 924(n) (firearms trafficking), 956 (conspiracy to kill, kidnap, maim, or injure certain property in a foreign country), 1005 (fraudulent bank entries), 1006 (fraudulent Federal credit institution entries), 1007 (fraudulent Federal Deposit Insurance transactions), 1014 (fraudulent loan or credit applications), *section 1030 (computer fraud and abuse)*, 1032 (concealment of assets from conservator, receiver, or liquidating agent of financial institution), 1111 (murder), 1114 (murder of United States law enforcement officials), 1116 (murder of foreign officials, official guests, or internationally protected persons), 1201 (kidnaping), 1203 (hostage taking), 1361 (willful injury of Government property), 1363 (destruction of property within the special maritime and territorial jurisdiction), 1708 (theft from the mail), 1751 (Presidential assassination), 2113 or 2114 (bank and postal robbery and theft), 2280 (violence against maritime navigation), 2281 (violence against maritime fixed platforms), 2319 (copyright infringement), 2320 (trafficking in counterfeit goods and services), *2332 (terrorist acts abroad against United States nationals), 2332a (use of weapons of mass destruction), 2332b (international terrorist acts transcending national boundaries)*, 2332g (missile systems designed to destroy aircraft), 2332h (radiological dispersal devices), or *section 2339A or 2339B (providing material support to terrorists)* of this title, section 46502 of title 49, United States Code, a felony violation of the Chemical Diversion and Trafficking Act of 1988 (precursor and essential chemicals), section 590 of the Tariff Act of 1930 (19 U.S.C. 1590) (aviation smuggling), 422 of the Controlled Substances Act (transportation of drug paraphernalia), 38(c) (criminal violations) of the Arms Export Control Act, 11 (violations) of the Export Administration Act of 1979, 206 (penalties) of the International Emergency Economic Powers Act, 16 (offenses and punishment) of the Trading with the Enemy Act, any felony violation of section 15 of the Food Stamp Act of 1977 [7 U.S.C.A. § 2024] (food stamp fraud) involving a quantity of coupons having a value of not less than $5,000, any violation of section 543(a)(1) of the Housing Act of 1949 [42 U.S.C.A. § 1490s(a)(1)] (equity skimming), any felony violation of the Foreign Agents Registration Act of 1938, any felony violation of the Foreign Corrupt Practices Act, or section 92 of the Atomic Energy Act of 1954 (42 U.S.C. 2122) (prohibitions governing atomic weapons)

"(E) a felony violation of the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), the Ocean Dumping Act (33 U.S.C. 1401 et seq.), the Act to Prevent Pollution from Ships (33 U.S.C. 1901 et seq.), the Safe Drinking Water Act (42 U.S.C. 300f et seq.), or the Resources Conservation and Recovery Act (42 U.S.C. 6901 et seq.); or

"(F) any act or activity constituting an offense involving a Federal health care offense;"18 U.S.C. 1956(c)(7)(emphasis added and repetitive use of the word "section" and phrase "related to" omitted)(sections in italics expire on December 31, 2005 by operation of section 224 of USA PATRIOT ACT, 18 U.S.C. 2510 note).

- with the intent to promote the theft of government property, wire fraud, or the interstate or foreign transportation or receipt of stolen property.
- or, knowing that the transaction's purpose is to conceal the proceeds of an illegal activity.[165]

Financial transactions are defined broadly to encompass virtually every possible transfer of wealth,[166] as long as they "in any way or degree affect[] interstate or foreign commerce . . . or . . . involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree," 18 U.S.C. 1956(c)(4). The proof required to satisfy this "any way or degree" jurisdictional element, even after *Lopez*, has been characterized as "de minimis," "minimal," "slight," or "incidental."[167]

---

[165] Or in the words of the statute "Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity – (A)(i) with the intent to promote the carrying on of specified unlawful activity or (B) knowing that the transaction is designed in whole or in part--(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or(ii) to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both," 18 U.S.C. 1956(a)(1).

[166] "(4) the term 'financial transaction' means (A) a transaction* which in any way or degree affects interstate or foreign commerce (i) involving the movement of funds by wire or other means or (ii) involving one or more monetary instruments,** or (iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or (B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree," 18 U.S.C. 1956(c)(4).

* "The term 'transaction' includes a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected," 18 U.S.C. 1956(c)(3).

** "The term 'monetary instruments' means (i) coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders, or (ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery," 18 U.S.C. 1956(c)(5).

[167] *United States v. Ables*, 167 F.3d 1021, 1029 (6th Cir. 1999); *United States v. Owens*, 167 F.3d 739, 755 (1st Cir. 1999); *United States v. Meshack*, 225 F.3d 556, 572 (5th Cir. 2000); *United States v. Oliveros*, 275 F.3d 1299, 1303 (11th Cir. 2001; *United States v. Ramerez*, 313 F. Supp. 2d 276, 279 (S.D.N.Y. 2004) In *United States v. Lopez*, 514 U.S. 549 (1995), the United States Supreme Court held that Gun Free School Zone Act, which purported to make it a federal crime to possess a gun in or near a school, failed to claim or exhibit the nexus to interstate or foreign commerce necessary to constitute the valid exercise of Congress' legislative authority under the Constitution's commerce clause.

To establish "promotion" the government need show little more than that the transaction is intended to further the illicit scheme, activity or business.[168]

"The elements necessary to prove a violation of §1957 are that:

(1) the defendant engage or attempt to engage
(2) in a monetary transaction
(3) in criminally derived property that is of a value greater than $10,000
(4) knowing that the property is derived from unlawful activity, and
(5) the property is, in fact, derived from 'specified unlawful activity.'"[169]

The predicate offenses are the same as those for section 1956, 18 U.S.C. 1957(f)(3), the meaning of "monetary transaction" closely tracks that of a "financial transaction" in section 1956,[170] and the definition of monetary transaction includes

---

[168] *United States v. Williamson*, 339 F.3d 1295, 1302 (11th Cir. 2003) (depositing and cashing checks of proceeds of fraud promoted present and future unlawful activities); *United States v. Rivera*, 295 F.3d 461, 469 (5th Cir. 2002)(bank withdrawal of a portion of the proceeds of a fraudulent scheme to pay a co-conspirator his share constituted "promotion"); see also, *United States v. Febus*, 218 F.3d 784, 790 (7th Cir. 1999) (operator of illegal gambling enterprise "promoted" the venture for money laundering purposes by paying off winning customers and thereby ensuring their continued patronage); *United States v. Meshack*, 225 F.3d 556, 573 (5th Cir. 2000)(defendant's use of drug money to pay the rent on his girlfriend's apartment where drugs were stored and which was used "in an attempt to conceal the conspiracy" was sufficient to establish promotion of the drug trafficking conspiracy); *United States v. Bockius*, 228 F.3d 305, 310 n.8 (3d Cir. 2000)(noting its holding in *United States v. Paramo*, 998 F.2d 1212, 1218 (3d Cir. 1993) (that a rationale jury could have concluded that cashing embezzled IRS checks was intended to promote the antecedent frauds).

[169] *United States v. Sokolow*, 91 F.3d 396, 408 (3d Cir. 1996); *United States v. Richard*, 234 F.3d 763, 767 (1st Cir. 2000); *United States v. Carucci*, 364 F3d 339,343 (1st Cir. 2004). Or more precisely, "(a) Whoever, in any of the circumstances set forth in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property that is of a value greater than $10,000 and is derived from specified unlawful activity, shall be punished as provided in subsection (b). "(b)(1) Except as provided in paragraph (2), the punishment for an offense under this section is a fine under title 18, United States Code, or imprisonment for not more than ten years or both. (2) The court may impose an alternate fine to that imposable under paragraph (1) of not more than twice the amount of the criminally derived property involved in the transaction.

"(c) In a prosecution for an offense under this section, the Government is not required to prove the defendant knew that the offense from which the criminally derived property was derived was specified unlawful activity.

"(d) The circumstances referred to in subsection (a) are – (1) that the offense under this section takes place in the United States or in the special maritime and territorial jurisdiction of the United States; or (2) that the offense under this section takes place outside the United States and such special jurisdiction, but the defendant is a United States person (as defined in section 3077 of this title, but excluding the class described in paragraph (2)(D) of such section). . ." 18 U.S.C. 1957(a)-(d).

[170] "As used in this section – (1) the term 'monetary transaction' means the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument (as defined in section 1956(c)(5) of this title) by, through, or to a

the jurisdiction component of the offense, that is, that the transaction occurs "in or affecting interstate or foreign commerce," 18 U.S.C. 1957(f)(1), which requires no more than the de minimis nexus demanded of section 1956.[171]

RICO. RICO follows a similar pattern. Any conduct that involves credit card fraud, wire fraud, the interstate transportation of stolen property or money laundering implicates federal Racketeer Influenced and Corrupt Organizations (RICO) provisions, 18 U.S.C. 1961-1965.[172] RICO outlaws the acquiring or conducting the business of a commercial enterprise through the patterned commission of predicate

---

financial institution (as defined in section 1956 of this title), including any transaction that would be a financial transaction under section 1956(c)(4)(B) of this title, but such term does not include any transaction necessary to preserve a person's right to representation as guaranteed by the sixth amendment to the Constitution," 18 U.S.C. 1957(f)(1).

[171] *United States v. Aramony*, 88 F.3d 1369, 1386 (4th Cir. 1996); *United States v. Kunzman*, 54 F.3d 1522, 1527 (10th Cir. 1995); it is enough, for example, for the government to show that the transaction involved a federally insured bank, *United States v. Benjamin*, 252 F.3d 1, 8 (1st Cir. 2001); *United States v. Ford*, 184 F.3d 566, 583-84 (6th Cir. 1999)*; United States v. Wadena*, 152 F.3d 831, 853 (8th Cir. 1998).

[172] See e.g., *General Motors Corp. v. Lopez de Arriortua*, 948 F.Supp. 670 (E.D.Mich. 1996)(civil RICO plaintiff charged with RICO violations based upon alleged acts of wire fraud and transportation of stolen property in interstate and foreign commerce, inter alia, in a case in which defendants allegedly transported computer disks containing plaintiff's trade secret information).

offenses[173] that include credit card fraud, wire fraud, and money laundering.[174] The

---

[173] "(a) It shall be unlawful for any person who has received any income derived, directly or indirectly, from a pattern of racketeering activity or through collection of an unlawful debt in which such person has participated as a principal within the meaning of section 2, title 18, United States Code, to use or invest, directly or indirectly, any part of such income, or the proceeds of such income, in acquisition of any interest in, or the establishment or operation of, any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce. A purchase of securities on the open market for purposes of investment, and without the intention of controlling or participating in the control of the issuer, or of assisting another to do so, shall not be unlawful under this subsection if the securities of the issuer held by the purchaser, the members of his immediate family, and his or their accomplices in any pattern or racketeering activity or the collection of an unlawful debt after such purchase do not amount in the aggregate to one percent of the outstanding securities of any one class, and do not confer, either in law or in fact, the power to elect one or more directors of the issuer.

"(b) It shall be unlawful for any person through a pattern of racketeering activity or through collection of an unlawful debt to acquire or maintain, directly or indirectly, any interest in or control of any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce.

"(c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt.

"(d) It shall be unlawful for any person to conspire to violate any of the provisions of subsection (a), (b), or (c) of this section," 18 U.S.C. 1962.

[174] Predicate offenses or "racketeering activities" as they are called in RICO are listed in 18 U.S.C. 1961(a)(1): "(A) any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), which is chargeable under State law and punishable by imprisonment for more than one year; (B) any act which is indictable under any of the following provisions of title 18, United States Code: Section 201 (bribery), 224 (sports bribery), 471, 472, and 473 (counterfeiting), 659 (theft from interstate shipment) if the act indictable under 659 is felonious, 664 (embezzlement from pension and welfare funds), 891-894 (extortionate credit transactions), 1028 (fraud and related activity in connection with identification documents), 1029 (fraud and related activity in connection with access devices), 1084 (the transmission of gambling information), 1341 (mail fraud), 1343 (wire fraud), 1344 (financial institution fraud), 1425 (the procurement of citizenship or nationalization unlawfully),1426 (the reproduction of naturalization or citizenship papers), 1427 (the sale of naturalization or citizenship papers), 1461-1465 (obscene matter), 1503 (obstruction of justice), 1510 (obstruction of criminal investigations), 1511 (the obstruction of State or local law enforcement), 1512 (tampering with a witness, victim, or an informant), 1513 (retaliating against a witness, victim, or an informant), 1542 (false statement in application and use of passport), 1543 (forgery or false use of passport), 1544 (misuse of passport), 1546 (fraud and misuse of visas, permits, and other documents), 1581-1591 (peonage, slavery, and trafficking in persons), 1951 (interference with commerce, robbery, or extortion), 1952 (racketeering), 1953 (interstate transportation of wagering paraphernalia), 1954 (unlawful welfare fund payments), 1955 (the prohibition of illegal gambling businesses), 1956 (the laundering of monetary instruments), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), 1958 (use of interstate commerce facilities in the commission of murder-for-hire), 2251, 2251A, 2252, and 2260 (sexual exploitation of children), 2312 and 2313 interstate transportation of stolen motor vehicles), 2314 and 2315 (interstate

offense condemns:

(1) any person
(2) who
    (a) invests in, or
    (b) acquires or maintains an interest in, or
    (c) conducts or participates in the affairs of, or
    (d) conspires to invest in, acquire, or conduct the affairs of
(3) an enterprise
(4) which
    (a) engages in, or
    (b) whose activities affect, interstate or foreign commerce
(5) through
    (a) the collection of an unlawful debt, or
    (b) the patterned commission of various state and federal crimes,
    18 U.S.C. 1962.

Violations are punishable by (a) forfeiture of any property acquired through a RICO violation and of any property interest in the enterprise involved in the violation, and (b) imprisonment for not more than 20 years, or life if one of the predicate offenses carries such a penalty, and/or a fine of not more than $250,000, 18 U.S.C. 1963.

RICO violations also subject the offender to civil liability. The courts may award anyone injured by a RICO violation treble damages, costs and attorneys' fees, and may enjoin RICO violations, order divestiture, dissolution or reorganization, or restrict an offender's future professional or investment activities, 18 U.S.C. 1964.

---

transportation of stolen property), 2318 (trafficking in counterfeit labels for phonorecords, computer programs or computer program documentation or packaging and copies of motion pictures or other audiovisual works), 2319 (criminal infringement of a copyright), 2319A (unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances), 2320 (trafficking in goods or services bearing counterfeit marks), 2321 (trafficking in certain motor vehicles or motor vehicle parts), 2341-2346 (trafficking in contraband cigarettes), 2421-24 (white slave traffic), 175-178 (biological weapons) , 229-229F (chemical weapons), 831 (nuclear materials), (C) any act which is indictable under title 29, United States Code, 186 (dealing with restrictions on payments and loans to labor organizations) or 501(c) (embezzlement from union funds), (D) any offense involving fraud connected with a case under title 11 (except a case under section 157 of this title), fraud in the sale of securities, or the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), punishable under any law of the United States, (E) any act which is indictable under the Currency and Foreign Transactions Reporting Act, (F) any act which is indictable under the Immigration and Nationality Act, section 274 (bringing in and harboring certain aliens), 277 (aiding or assisting certain aliens to enter the United States), or 278 (relating to importation of alien for immoral purpose) if the act indictable under such section of such Act was committed for the purpose of financial gain, or (G) any act that is indictable under any provision listed in section 2332b(g)(5)(B).”(repetitive use of the word “section” and phrase “related to” omitted). Commentaries include, *Nineteenth Survey of White Collar Crime: Racketeer Influenced and Corrupt Organizations*, 41 AMERICAN CRIMINAL LAW REVIEW 1027 (2004).

The money laundering provisions can also serve as a bridge to RICO. For example, the theft of federal property, 18 U.S.C. 641, is a money laundering predicate offense. Theft of federal property is not a RICO predicate, but money laundering is, 18 U.S.C. 1956(c)(7), 1961(1). Thus, anyone guilty of stealing federal property who either deposits the proceeds in a financial institution (assuming they amount to more than $10,000) or who churns the proceeds back into a scheme to steal federal property is guilty of money laundering, 18 U.S.C. 1956, 1957. Anyone who engages in a pattern of such money laundering activities in order to acquire or conduct the affairs of commercial enterprise is guilty of a RICO violation, 18 U.S.C. 1962. And thus in a sense section 641 becomes a RICO predicate by way of money laundering.

Travel Act. Money laundering also acts as a bridge to the Travel Act and from there to RICO. The Travel Act, 18 U.S.C. 1952, in relevant part, bars anyone from using any facility in interstate or foreign commerce to "promote" the money laundering.[175] Thus, money laundering is a Travel Act predicate and any crime that constitutes a money laundering predicate, 18 U.S.C. 1956(C)(7), may become a Travel Act predicate, e.g., various paragraph 1030(a)(4) computer companion offenses such as crimes under 18 U.S.C. 1343 (mail fraud); 641 (theft of government property); 2314 (interstate transportation of stolen property), 1029 (credit card fraud).

State computer fraud law. Although the elements vary considerably, most states have explicit statutory prohibitions against computer fraud.[176]

---

[175] "(a) Whoever travels in interstate or foreign commerce or uses the mail or any facility in interstate or foreign commerce, with intent to – (1) distribute the proceeds of any unlawful activity [i.e., "any act which is indictable under [18 U.S.C.] 1956 or 1957 " (18 U.S.C. 1952(b)(3))]; . . . or (3) otherwise promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on, of any unlawful activity, and thereafter performs or attempts to perform – (A) an act described in paragraph (1) or (3) shall be fined under this title, imprisoned not more than 5 years, or both," 18 U.S.C. 1952.

[176] ALA.CODE §§13A-8-102, 13A-8-103; ALASKA STAT. §11.46.740; ARIZ.REV. STAT.ANN. §13-2316, 2316.02; ARK.CODE ANN. §5-41-103; CAL.PENAL CODE §502; COLO.REV. STAT.ANN. §18-5.5-102; CONN.GEN.STAT.ANN. §53a-251; FLA.STAT. ANN. §815.04; GA.CODE ANN. §16-9-93, 93.1; HAWAII REV.STAT. §708-891, 891.5; IDAHO CODE §18-2202; ILL. COMP.STAT.ANN. 720 5/16D-5; KAN.STAT.ANN. §21-3755; KY.REV.STAT.ANN. §434.845-855; LA. REV.STAT.ANN. §14:73.5; GA.CODE ANN. §§16-9-93, 16-9-93.1; ME. REV.STAT.ANN. tit.17-A §433; MASS.GEN.LAWS ANN. Ch.266, §30; MICH.COMP.LAWS ANN. §752.794; MINN.STAT.ANN. §609.89; MISS. CODE ANN. §97-45-3; MONT.CODE ANN. §45-6-311; NEB.REVSTAT. §28-1344; NEV.REV. STAT. 205.4765, 481; N.H.REV.STAT.ANN. §638:17; N.J.STAT.ANN. §§2C:20-25, 2A:38 A-3; N.MEX.STAT.ANN. §30-45-3; N.Y. PENAL LAW §§156.10 to 156.27; N.C.GEN.STAT. §14-454, 458; N.D. CENT.CODE §12.1-06.1-08; OKLA.STAT.ANN. tit.21 § 1953, 1958; ORE.REV.STAT. §164.377; PA.STAT.ANN. tit.18 §1711; R.I.GEN.LAWS §11-52-2; S.C. CODE ANN. §16-16-20; S.D.COD.LAWS §43-43B-1; TENN.CODE ANN. §39-14-602; TEX.PENAL CODE ANN. §33.02; UTAH CODE ANN. §76-10-1801; VT.STAT.ANN. tit.13 §4105; VA.CODE §18.2-152.3; WASH. REV.CODE ANN. §9A.52.110; W.VA.CODE ANN. §61-3C-4; WIS.STAT.ANN. §943.70; WYO.STAT. §6-3-502.

Extortionate Threats
18 U.S.C. 1030(a)(7)

> *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.*

Congress added paragraph 1030(a)(7) in 1996 out of concern that "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 threat to injury 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. 357 at 12. The paragraph provides that no one shall

- transmit in interstate or foreign commerce
- any communication containing any threat
- to cause damage, [i.e., "any impairment to the integrity or availability of data, a program, a system, or information," (1030(e)(8))]
- to a protected computer, [i.e. one
  - used exclusively for or by the federal government;
  - used exclusively for or by a bank or other financial institution;
  - used in part for or by the federal government where the damage would "affect" government use or use of the government's behalf;
  - used in part for or by a bank or other financial institution where the damage would "affect" use by or on behalf of the institution; or
  - used in interstate or foreign commerce or communications (1030(e)(2))]
- with the intent to extort money or a thing of value
- from any person [i.e. any individual, firm, association, educational institution, financial institution, government entity, legal or other entity (1030(3)(12))].

Violations are punishable by imprisonment for not more than 5 years (not more than 10 years for second and subsequent offenses) and/or a fine of not more than $250,000, and in cases involving more than $5000 damage or some other qualifying circumstance, victims may claim the advantages of the civil cause of action for

damages available under 18 U.S.C. 1030(g).[177] Other possible consequences include confiscation and restitution orders, 18 U.S.C. 981, 982, 3663.

Jurisdiction.

Paragraph 1030(a)(7) stands on dual jurisdictional footings. First, a successful prosecution is only possible if a threat with intent to extort has been transmitted in interstate or foreign commerce, an element that may be satisfied even in the case of intrastate communications under some circumstances.[178] Second, conviction can only be had if the transmitted threat is directed against a protected computer, i.e., one used in or for interstate or foreign commerce, one used by or for the federal government, or one used by or for a financial institution, 18 U.S.C. 1030(e)(2).

Threat of "damage".

Paragraph 1030(a)(7) proscribes threats to cause computer "damage" and the legislative history describes its reach in terms consistent with the common understanding of the word "damage":

> "New section 1030(a)(7) would close [the] gap in the law and provide penalties for the interstate or international transmission of threats directed against computers and computer systems. This 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 massaging service. *Unlawful threats could include interference 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, slowing down the operation of the computer or system, or encrypting data and then demanding money for the key," S.Rep.No. 357 at 12 (emphasis added).

Prior to the USA PATRIOT Act amendments, the paragraph did not cover all threats to interfere with the normal operation of protected computers, but only threats to "damage" protected computers and only "damage" as then defined in section 1030, i.e., "any impairment to the integrity or availability of data, a program,

---

[177] ". . . A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B) . . ." 18 U.S.C. 1030(g). The qualifying circumstances described in clauses (a)(5)(B)(i) through (v) are: "(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security."

[178] See e.g., *United States v. Kammersell*, 196 F.3d 1137, 1138-140 (10th Cir. 1999)(a threat communicated between two computers in Utah involved interstate communications because the communications was forwarded by way of AOL's server in Virginia).

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," 18 U.S.C. 1030(e)(8)(2000 ed.). The Act expanded the damage definition and thus the coverage of the paragraph by reducing the definition to "any impairment to the integrity or availability of data, a program, a system, or information," 18 U.S.C. 1030(e)(8).

Intent.

The level of intent required for a violation of paragraph 1030(a)(7) differs from the level used for the fraud provisions of section 1030. Rather than the demand that the offense be committed "knowingly and with an intent to defraud;" offenses under paragraph 1030(a)(7) must be committed "with the intent to extort." Because the crime is only complete if committed with this intent to extort, it anticipates that the offender will have intended his victim to feel threatened. The paragraph thereby avoids some of the uncertainty that has plagued the threat statutes.[179]

Threats.

Construction of the threat statutes may provide useful insight, however, into what constitutes a "threat" for purposes of paragraph 1030(a)(7). Although statements of political hyperbole may not always constitute true threats,[180] a threat is

---

[179] The circuits are divided over the question of whether in order to convict under some of the threat statutes, the government must show that the defendant intended the victim to feel threatened or merely intended the conduct that a reasonable person would consider threatening. *United States v. Darby*, 37 F.3d 1059, 1963-66 (4th Cir. 1994)(and the conflicting cases cited there)("to establish a violation of section 875(c) the government must establish that the defendant intended to transmit the interstate communication and that the communication contained a true threat. . . . The government does not have to prove that the defendant subjectively intended for the recipient to understand the communication as a threat"); *United States v. Alkhabaz (Baker)*, 104 F.3d 1492, 1495 (6th Cir. 1997)("to constitute a communication containing a threat under Section 875(c), a communication must be such that a reasonable person (1) would take the statement as a serious express of an intention to inflict bodily harm (the mens rea), and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the actus reus)"); *United States v. Stewart*, __F.3d__, 2005 WL 1389434, at *3 (7th Cir. June 14, 2005)("guilt is not dependent upon what the defendant intended, but whether the recipient could reasonably have regarded the defendant's statement as a threat")(court declines to follow contradictory Ninth Circuit precedent)(Id. at *7n4).

[180] *United States v. Hinkson,* 349 F.Supp.2d 1350 ("Certain expressions, including 'vehement, caustic, and sometimes unpleasantly sharp attacks on Government and public officials[,]' may be protected free speech")(citing *Watts v. United States*, 394 U.S. 705, 708 (1969)). Moreover, "generally, a person who informs someone that he or she is in danger from a third party has not made a threat," *New York ex rel. Spitzer v. Operation Rescue National*, 273 F.3d 184, 196 (2d Cir. 2001).

no less a threat because it is contingent, [181] because the speaker does not intend or is unable to carry it out,[182] because the threat was not directly communicated to the target[183], or because the language used might be considered cryptic or ambiguous.[184] Whether a particular communication constitutes a threat is a question determined by whether a reasonable person, considering all the circumstances, would regard the communication as a threat.[185] While the jurisdictional element, such as transmission in interstate commerce, must be established,[186] the government need not show the defendant knew that the threat had been transported interstate commerce.[187]

Penalties.

Violations of paragraph 1030(a)(7) are punishable by imprisonment for not more than 5 years (not more than 10 years for second and subsequent offenses) and/or a fine of not more than $250,000, 18 U.S.C. 1030(c)(3), 3571. The general fraud/damage sentencing guideline, U.S.S.G. §2B1.1, applies to violations of paragraph (a)(7). As with other violations of section 1030, offenders may be subject to civil suit for damages, 18 U.S.C. 1030(g).

---

[181] *United States v. Patrick*, 117 F.3d 375, 377 (8th Cir. 1997)("that Patrick's threat was contingent upon his release from prison does not save him from violating section 876"); *United States v. Viefhaus*, 168 F.3d 392, 396 (10th Cir. 1999); as the phrase "your money or your life" demonstrates, contingent threats are an essential component of robbery and extortion.

[182] *United States v. Cassel*, 408 F.3d 622, 627-28 (9th Cir. 2005);*United States v. Saunders*, 166 F.3d 907, 914 (7th Cir. 1999); *United States v. Martin*, 163 F.3d 1212, 1216 (10th Cir. 1998).

[183] *United States v. Hinkson*, 349 F. Supp. 2d 1350, 1355 (D. Idaho 2004).

[184] *United States v. Fulmer*, 108 F.3d 1486, 1492 (1st Cir. 1997); *United States v. Malik*, 16 F.3d 45, 49 (2d Cir. 1994).

[185] *United States v. Aman*, 31 F.3d 550, 553-55 (7th Cir. 1994); *United States v. Francis*, 164 F.2d 120, 123 (2d Cir. 1999); *United States v. Morales*, 272 F.3d 284, 287 (5th Cir. 2001). *United States v. Stewart*, __F.3d__, 2005 WL 1389434, at *3 (7th Cir. June 14, 2005) ("the government must prove that the statement came in a context or under such circumstances wherein a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates a statement as a serious expression of an intention to inflict bodily harm upon or to take the life of [another individual].")

[186] *United States v. Korab*, 893 F.2d 212, 214-15 (9th Cir. 1989).

[187] *United States v. Darby*, 37 F.3d at 1063-64; see also, *United States v. Kammersell*, 196 F.3d 1137, 1139-140 (10th Cir. 1999)(a threatening computer message from defendant in Utah to his girlfriend's place of employment within the same state constituted transmission of a threatening communication in interstate commerce because the message was transmitted by way of the defendant's service provider's main server in Virginia; see also *United States v. Guerva*, 408 F.3d 252, 259 (5th Cir. 2005)(court finding that threat that led to the temporary closing of a federal building and the shutting down of various federal agencies resulted in threat affecting interstate commerce).

Other crimes.

Attempt, conspiracy and complicity.

The same general observations concerning attempt, conspiracy and aiding and abetting noted with respect to the other paragraphs of 1030(a) apply here. It is a separate crime to attempt to violate paragraph 1030(a)(7), 18 U.S.C. 1030(b). Those who attempt or aid and abet the violation of another are subject to the same penalties as those commit the substantive offense, 18 U.S.C. 1030(c), 2. The same is true of conspiracies except that conspiracy to commit a felony carries a 5 year maximum of imprisonment, 18 U.S.C. 371.

Hobbs Act.

The Hobbs Act, 18 U.S.C. 1951, prohibits extortion that affects commerce. More precisely, among other things, it declares that "Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by . . . extortion or attempts or conspires so to do . . . shall be fined under this title or imprisoned not more than twenty years, or both," 18 U.S.C. 1951(a).[188] For purpose of section 1951, "'extortion' means the obtaining of property from another, with his consent, induced by wrongful use of . . . fear," 18 U.S.C. 1951(b)(2). The government need show only a minimal impact on interstate or foreign commerce to satisfy the jurisdictional element of the Hobbs Act.[189]

Facially paragraph 1030(a)(7) might seem little more than a more specific version of the Hobbs Act: the Hobbs Act prohibits extortionate acquisition of property, generally, in a manner that affects interstate or foreign commerce; while paragraph 1030(a)(7) prohibits extortionate acquisition of property, specifically acquired by a threat to damage computers, in a manner that affects interstate or foreign commerce. But much of section 1030 can be explained by Congress' concern that its purposes could be frustrated by too narrow a definition of "property." In most instances, the fear has been that computer systems or information in computer storage or on computer disks will be considered too intangible to claim the legal protection available to more tangible property. The applicability of the Hobbs Act and of the various "threats with intent to extort" statutes present an additional "property" complication, for they may involve both property under threat and property sought by the extortionist.

---

[188] For a general discussion see, *Elements of Offense Proscribed by the Hobbs Act (18 USCS §1951) Against Racketeering in Interstate or Foreign Commerce*, 4 ALR FED. 881 (2005).

[189] *United States v. Vega Molina*, 407 F.3d 511, 526 (1st Cir 2005); *United States v. Vallejo*, 297 F.3d 1154, 1166 (11th Cir. 2002); *United States v. Peterson*, 236 F.3d 848, 852-53 (7th Cir. 2001); *United States v. Malone*, 222 F.3d 1286, 1294-295 (10th Cir. 2000). Some circuits may be more demanding where the victim is an individual rather than a business, *United States v. Lynch*, 282 F.3d 1049, 1052-55 (9th Cir. 2002) (requiring greater commerce showing the case of individual victims and describing views of other circuits).

There is little question that the Act guards against threats to both tangible and intangible property. The cases are replete with the observation that wrongful exploitation of a reasonable fear of economic loss in order to obtain property constitutes extortion for purposes of section 1951.[190] The case law gives credence to Congress' concern that some may conclude that the Hobbs Act does not always reach cases where the "property" obtained by the extortionist is an intangible benefit rather than tangible property like money.[191]

Threat statutes.

Several federal statutes prohibit threats against "property" made with extortionate intent. Here the Hobbs Act puzzle is reversed. Here it is the meaning of the "property" protected from threat that is uncertain; while the meaning of "property" sought by the extortionist is conceded and spacious.

The statutes in questions include at a minimum 18 U.S.C. 875 (threats transmitted in interstate commerce),[192] 18 U.S.C. 876 (mailing threatening

---

[190] *United States v. Cruzado-Laureano*, 404 F.3d 470, 481 (1st Cir. 2005);*United States v. Edwards*, 303 F.3d 606, 635 (5th Cir. 2002); *United States v. Collins*, 78 F.3d 1021, 1029-30 (6th Cir. 1996); *United States v. Middlemiss*, 217 F.3d 112, 118 (2d Cir. 2000).

[191] Compare, *National Organization for Women, Inc. v. Scheidler*, 267 F.3d 687, 709 (7th Cir. 2001), rev'd, 537 U.S. 393 (2003)(rejecting a contention that neither women's right to receive medical services from abortion clinics nor the clinics' right to provide such services constituted "property" received under threat for Hobbs Act purposes), and *United States v. Gigante*, 39 F.3d 42, 49-51 (2d Cir. 1994)(holding that the Act extended to a benefit realized when the victim of the threat agreed not to engage in competition bidding on a public contract against with firms paying kickbacks to the extortionists); with, *Town of West Hartford v. Operation Rescue*, 915 F.2d 92, 101-2 (2d Cir. 1990)(despite recognition that "'property' under the [Hobbs] Act 'includes in a broad sense, any valuable right considered as a source or element of wealth' including a right to solicit business . . . the term 'property' cannot plausible be construed to encompass altered official conduct," i.e., increased police and other emergency services), and *United States v. Edwards*, 303 F.3d 606, 635 (5th Cir. 2002)(noting that the "property" threatened for Hobbs Act purposes does not include potential benefits or opportunities). The Supreme Court subsequently resolved the Hobbs Act issue – not by determining whether the extraction of intangible property is sufficient to constitute extortion under the Act – but by concluding that the Hobbs extortion requires that the offender "obtain" something, merely compelling the victim to forego the exercise of a prerogative is insufficient, *Scheidler v. National Organization for Women, Inc.*, 537 U.S. 393, 402-10 (2003). For a discussion on the Hobbs Act in relation to social protest activity and the meaning of property in that context, see Kristal S. Stippich, *Behind the Words: Interpreting the Hobbs Act requirement of "obtaining of property from another*" 36 JOHN MARSHALL LAW REVIEW 295 (2003).

Congress' uncertainty notwithstanding, at least one district court has confirmed the extraterritorial application of the Hobbs Act, 18 U.S.C. 371 (conspiracy), 18 U.S.C. 1029 (access device offenses), as well as paragraphs 1030(a)(7)(extortion) and 1030(a)(4)(fraud) to misconduct arising out of an overseas extortionate threat against a commercial computer system in this country, *United States v. Ivanov*, 175 F.Supp.2d 367 (D.Conn. 2001).

[192] "Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property . . . of the addressee or of

communications),[193] 18 U.S.C. 877 (mailing threatening communications from a foreign country),[194] and 18 U.S.C. 880 (receipt of the proceeds of extortion).[195] Other than the receipt statute, they are all essentially alike except for their jurisdictional elements. Each prohibits the communication of a threat to injure the property of the addressee or of another conveyed with extortionate intent. Each identifies "money or other thing of value" as the extortionist's objective, and each punishes offenders by imprisonment for not more than two years and/or a fine of not more than $250,000.

As noted earlier, the courts see extraordinary elasticity in the term "thing of value" as used in federal criminal law,[196] but not infrequently are divided over which intangibles may legitimately be considered "property" for purposes of federal criminal statutes.[197] Again even in the case of the "property" statutes, however, the

---

another. . . shall be fined under this title or imprisoned not more than two years, or both," 18 U.S.C. 875(d).

[193] "Whoever, with intent to extort from any person any money or other thing of value, knowingly so deposits or causes to be delivered, as aforesaid, any communication, with or without a name or designating mark subscribed thereto, addressed to any other person and containing any threat to injure the property . . . of the addressee or of another . . . . shall be fined under this title or imprisoned not more than two years, or both. If such a communication is addressed to a United Stats judge, a federal law enforcement officer, or an official who is covered by section 1114 [any federal employee], the individual shall be fined under this title, imprisoned not more than 10 years, or both," 18 U.S.C. 876(d).

[194] ". . . Whoever, with intent to extort from any person any money or other thing of value, knowingly so deposits as aforesaid, any communication, for the purpose aforesaid, containing any threat to injure the property . . . of the addressee or of another . . . shall be fined under this title or imprisoned not more than two years, or both," 18 U.S.C. 877.

[195] "A person who receives, possesses, conceals, or disposes of any money or other property which was obtained from the commission of any offense under this chapter that is punishable by imprisonment for more than 1 year, knowing the same to have been unlawfully obtained, shall be imprisoned not more than 3 years, fined under this title, or both," 18 U.S.C. 880.

[196] See, *United States v. Maneri,* 353 F.3d 165, 168 (2d Cir. 2003)(thing of value included opportunity for sexual encounter);*United States v. Freeman*, 208 F.3d 332, 341 (1st Cir. 2000)(night club owner's special treatment of police officer including access to dancers' dressing room constituted a thing of value); *United States v. Marmolejo*, 89 F.3d 1185, 1192-193 (5th Cir. 1996)(citing a wide range of intangible property benefits found to constitute "things of value" under various federal criminal statutes); *United States v. Bryant*, 117 F.3d 1464, 1468 n.7 (D.C.Cir. 1997)(noting that a forbearance from arrest constitutes a "thing of value" for purposes of 18 U.S.C. 912 even in a case where two members of the three judge panel expressed the view that the defendant should never have been charged, prosecuted or convicted); *United States v. Collins*, 56 F.2d 1416, 1420 (D.C.Cir. 1995)(noting the widespread acceptance of an expansive reading of the term "thing of value" the purposes of the theft of federal property statute, 18 U.S.C. 641).

[197] *United States v. Salvatore*, 110 F.3d 1131, 1139-141 (5th Cir. 1997)(noting the *McNally-Carpenter* distinction and the split of appellate courts on the question of whether unissued licenses may constitute "property" interests for purposes of the mail fraud statute, 18 U.S.C. 1341, a conflict which the Supreme Court subsequently resolved in *Cleveland v. United States*, 531 U.S. 12, 26-7 (2000) when it concluded that a state had not been

intangibles at issue in computer cases would seem to fall more clearly on the *Carpenter* "confidential information" side of the line than on the *McNally* "honest public services" or the *Cleveland* "unissued license" side.

RICO, money laundering, & the Travel Act.

Section 1030 is a money laundering predicate offense, 18 U.S.C. 1956(c)(7)(D), 1957(f)(3), and the money laundering proscriptions are RICO predicates, 18 U.S.C. 1961(1). Thus, financial transactions involving the proceeds from computer-related extortion that violates paragraph 1030(a)(7) may support a prosecution under 18 U.S.C. 1956 or 1957. If so they may also support a RICO prosecution. Moreover, a violation of paragraph 1030(a)(7) may at the same time offend one of its companions that is another RICO predicate, e.g., the Hobbs Act, 18 U.S.C. 875 (extortion affecting in interstate or foreign commerce), or the Travel Act (extortion is a Travel Act predicate), thereby rising the prospect of a RICO prosecution on other grounds.

Trafficking in Computer Access 18 U.S.C. 1030(a)(6)

> *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.*

Paragraph 1030(a)(6) outlaws misconduct similar to the access device proscriptions of section 1029.[198] It was enacted to deal with the practice of hackers of posting the passwords of various computer systems on electronic bulletin boards, S.Rep.No. 99-432 at 13 (1986); H.R.Rep.No. 99-612 at 12-3 (1986). Although limited, it provides several distinct advantages. First, it covers passwords to government computers more clearly than does section 1029. Second, as something

---

defrauded of "property" for the purposes of section 1341 when it was fraudulently induced by issue a license); *United States v. Delano*, 55 F.3d 720, 726-27 (2d Cir. 1995)(holding that labor or services cannot be considered "property" for purposes of a RICO charged based on an extortionate predicate offense). *United States v. Hedaithy*, 392 F.3d 580, 584 (3d Cir. 2004) (court found that mail fraud violation occurred when would-be test takers had others take a standardized test in their place; the court found that the testing service's property interests were violated because of the unauthorized use of its copyrighted and confidential materials and because, in obtaining a score report, the defendants possessed the "embodiment of the services that ETS provides").

198 "Whoever . . . knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section," 18 U.S.C. 1029(a)(2). Violations are punishable by imprisonment for not more than 10 years and/or a fine of not more than $250,000, 18 U.S.C. 1029(c)(1).

of a lesser included offense to section 1029, it affords the government plea bargain room in a case that it might otherwise be forced to bring under section 1029 or abandon. Third, it contributes a means of cutting off the practice of publicly posting access to confidential computer systems without imposing severe penalties unless the misconduct persists. Fourth, it supplies a basis for private enforcement through the civil liability provisions of subsection 1030(g) for misconduct that may be more appropriately addressed by the courts as a private wrong. The elements of the crime are:

- knowingly and with an intent to defraud;
- trafficking in (i.e. "to 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 computer password or similar computer key; and
- either
  - of a federal computer or
  - in a manner that affects interstate or foreign commerce.

Jurisdiction.

Federal jurisdiction exists where the traffic affects interstate or foreign commerce, 18 U.S.C. 1030(a)(6)(A) or where the password or key is to a computer used by or for the Government of the United States, 18 U.S.C. 1030(a) (6)(B). As has been said of other paragraphs and government computers, it is unclear whether the protection of paragraph 1030(a)(6) cloaks legislative and judicial branch computers or is limited to those of the executive branch. The uncertainty is born of the section's care to define the phrase "department or agency of the United States" to include all three branches and its use of that phrase in establishing some crimes, contrasted with its failure to use that phrase in paragraph 1030(a)(6), discussed *supra*.

Intent.

The intent element is the same as that used in paragraph 1030(a)(4)(fraud), and in the credit card fraud proscriptions of 18 U.S.C. 1029: knowingly and with the intent to defraud, S.Rep.No. 99-432 at 10 (1986); H.R.Rep.No. 99-612 at 12 (1986). The phrase as used in the credit card fraud statute means that the offender is conscious of the natural consequences of his action (i.e., that it likely that someone will be defrauded) and intends that those consequences should occur (i.e., he intends that someone should be defrauded), H.R.Rep.No. 98-894 at 16-7 (1984).

Penalties.

The first offense is punishable by imprisonment for not more than 1 year and/or a fine of not more than $100,000; subsequent offenses are punishable by imprisonment for not more than 10 years and/or a fine of not more than $250,000, 18 U.S.C. 1030(c)(2); 18 U.S.C. 3571. The general theft/damage sentencing guideline, U.S.S.G. §2B1.1, covers violations of paragraph 1030(a)(6)(traffic in

passwords) as it does fraud and damage under paragraphs 1030(a)(4) and 1030(a)(5). Offenders may also be civilly liable to their victims, if the requirements of 18 U.S.C 1030(g) are met.[199]

Other crimes.

The generally applicable provisions dealing with attempt, conspiracy and complicity will apply with equal force in cases involving paragraph 1030(a)(6). Paragraph 1030(a)(6) appears to have few counterparts in federal law, other than the prohibition against trafficking in access devices (credit card fraud) under 18 U.S.C. 1029(a)(2) [200] and the wire fraud provisions of 18 U.S.C. 1343.[201] Nevertheless, violations of either of these – or of the money laundering proscriptions (18 U.S.C. 1956, 1957) for which section 1030 is a predicate – may provide the foundation for a RICO (18 U.S.C. 1962) prosecution, so that should conduct in violation of paragraph 1030(a)(6) also offend either the mail fraud, credit card fraud or money laundering prohibitions, a criminal breach of RICO may also have occurred. Brokering computer passwords without more may not be the ground upon which a sprawling criminal enterprise might be built, but violations of paragraph 1030(a)(6), with other crimes, might be part of a pattern of criminal activity used to operate such an enterprise.

Computer Espionage 18 U.S.C. 1030(a)(1)

> *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*

---

[199] "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware," 18 U.S.C. 1030(g).

[200] Prosecution under paragraph 1029(a)(2) requires a loss of at least $1,000 over the course of a year and that the device permit access to an "account," 18 U.S.C. 1029(e)(1)(defining "access device"); paragraph 1030(a)(6) imposes neither burden upon a prosecution. This is probably why paragraph 1030(a)(6) is punishable as a misdemeanor while paragraph 1029(a)(2) is a 10 year felony.

[201] To establish wire fraud, the government must show an interstate wire transmission in furtherance of a scheme to defraud another of money or property, *United States v. Dowlin,* 408 F.3d 647, 658 n.5 (10th Cir. 2005)*; United States v. Owens*, 301 F.3d 521, 528 (7th Cir. 2002); *United States v. Rivera*, 295 F.3d 461, 466 (5th Cir. 2002).

> *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.*

Paragraph 1030(a)(1) essentially tracks existing federal espionage laws, 18 U.S.C. 793, 794 and 798, that ban disclosure of information potentially detrimental to our national defense and well being, or more simply laws that outlaw spying.[202] The paragraph was enacted as part of the original act and has been amended primarily to more closely track other espionage laws.[203] The distinctive feature of paragraph 1030(a)(1) is its merger of elements of espionage and computer abuse.[204] Broken down into a simplified version of its constituent elements it bars anyone from:

- either
- willfully disclosing,
- willfully attempting to disclose, or
- willfully failing to return

---

[202] For a discussion of federal espionage laws generally see, 70 AMERICAN JURISPRUDENCE, 2D EDITION, *Sedition, Subversive Activities, and Treason* §§17-44; see also, Bazan, *Espionage and the Death Penalty*, 41 FEDERAL BAR NEWS & JOURNAL 615 (1994).

[203] 18 U.S.C. 1030 (1982 ed. & 1984 Supp.); H.R.Rep.No.98-894 at 21 (1984). Compare the language of 1030(a)(1) with that of 18 U.S.C. 793(e)("Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe 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").

[204] "Although there is considerable overlap between 18 U.S.C. 793(3) and section 1030(a)(1), as amended by the NII Protection Act, the two statutes would not reach exactly the same conduct. Section 1030(a)(1) wold target those persons who deliberately break into a computer to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of Government secrets to foreign agents, 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. In this sense then, it is the use of the computer which is being proscribed, not the unauthorized possession of, access to, or control over the classified information itself," S.Rep.No. 104-357 at 6-7.

- classified information concerning national defense, foreign relations or atomic energy

- with reason to believe that the information either
- could to used to injure the United States, or
- could be used to the advantage of the a foreign nation

- when the information was acquired by unauthorized computer access.

Jurisdiction.

The federal government is a creature of the Constitution. It enjoys only those powers that the Constitution grants it, U.S.Const. Amend. IX, X. Since states are primarily responsible for the enactment and enforcement of criminal law, the validity of any federal criminal law depends upon a clear nexus some power that the Constitution vests in the national government. Most of section 1030 represents the execution of Congress' authority to enact laws for the regulation interstate and foreign commerce, for example, U.S.Const. Art.I, §8, cl.3. Paragraph 1030(a)(1), on the other hand, is anchored in the protection of defense and foreign relations of the nation and so jurisdictional ties to interstate or foreign commerce are unnecessary.

Intent.

The state of mind element for a breach of paragraph 1030(a)(1) is pegged high. The offender must (1) purposefully transmit or retain information that (2) he has reason to believe could be used to the injure the United States or benefit another country, and (3) that he has obtained through access to a computer that he knows he had no authority to access.[205]

Penalties.

Violations are punishable by imprisonment for not more than 10 years (not more than 20 years for second and subsequent offenses) and/or a fine of not more than $250,000, 18 U.S.C. 1030(c)(1), 3571. The general espionage sentencing guideline, U.S.S.G. §2M3.2, applies to violations of paragraph (a)(1) which calls for a base sentencing level of 30 (carrying an initial sentencing range beginning at 8 years imprisonment) and of 35 (an initial sentencing range beginning at 14 years) if top secret information is involved. Offenders may also be subject to a cause of action for damages or injunctive relief, 18 U.S.C. 1030(g).

---

[205] H.R.Rep.No. 98-894 at 21 (1984)("As the Supreme Court stated in *Gorin v. U.S.*, (312 U.S. 19, 28), 'This requires those prosecuted to have acted in bad faith. The sanctions apply only when scienter is established'").

Other crimes.

Espionage prosecutions are not common.[206] And there do not appear to have been any reported cases brought under paragraph 1030(a)(1). The overlap between paragraph 1030(a)(1) and the espionage laws is such, however, that any case prosecutable under paragraph 1030(a)(1) would like also be prosecutable under one or more of the espionage statutes; in fact "the only reported 'espionage' case involving the unauthorized use of computers was prosecuted under §793, the much older, pre-electronic espionage statute and not under §1030(a)(1)."[207]

Attempt, conspiracy, and complicity.

Subsection 1030(b) makes it a separate crime to attempt to commit a violation of paragraph 1030(a)(1) punishable to the same extent as the underlying offense, 18 U.S.C. 1030(c). Anyone who commands, counsels, aids or abets a violation of the paragraph assumes is as a principal and is therefore likewise subject to the same penalties, 18 U.S.C. 2. Conspirators to violate paragraph 1030(a)(1) are subject to imprisonment for not more than 5 years and/or a fine of not more than $250,000, 18 U.S.C. 371, and are each liable for the underlying offense and any other foreseeable crimes committed in furtherance of the conspiracy.

Espionage offenses.

The three espionage statutes themselves share common ground under some circumstances. In general terms, they outlaw gathering and disseminating defense information (18 U.S.C. 793), gathering and disseminating defense information for a foreign country (18 U.S.C. 794), and disclosing classified information concerning government cryptography or communications intelligence (18 U.S.C. 798).

As already noted 18 U.S.C. 793(e) is the generic twin of 1030(a)(1), but section 793 has several other provisions that might also be implicated by a fact pattern sufficient to establish criminal liability under paragraph 1030(a)(1). Section 793 establishes six distinct offenses:

- intruding upon military facilities to gather national defense information (18 U.S.C. 793(a));[208]

---

[206] See generally, Cavanagh & Flagg, *Espionage in the United States: Individuals Arrested 1993-1998* CRS REP. No. 97-805 GOV (April 23, 1998); Cavanagh, *Individuals Arrested on Charges of Espionage Against the United States Government*, CRS REP. No. 93-531 GOV (May 27, 1993).

[207] Olivenbaum, *<CTRL><ALT><DELETE>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL LAW REVIEW 574, 594-95 (1997), citing *United States v. Poulsen*, 41 F.3d 1330 (9th Cir. 1994).

[208] "Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal,

• copying documents containing national defense information (18 U.S.C. 793(b));[209]

• unlawful receipt of national defense information (18 U.S.C. 793(c));[210]

• unlawful dissemination of national defense information by a lawful custodian (18 U.S.C. 793(d));[211]

• unauthorized possession of national defense information (18 U.S.C. 793(e)); [212] and

• negligently losing national defense information (18 U.S.C. 793(f)).[213]

---

railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense . . . Shall be fined under this title or imprisoned not more than ten years, or both," 18 U.S.C. 793(a).

[209] "Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense . . .Shall be fined under this title or imprisoned not more than ten years, or both,"18 U.S.C. 793(b).

[210] "Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter . . . Shall be fined under this title or imprisoned not more than ten years, or both,"18 U.S.C. 793(c).

[211] "Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe 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 on demand to the officer or employee of the United States entitled to receive it . . . Shall be fined under this title or imprisoned not more than ten years, or both,"18 U.S.C. 793(d).

[212] Text at note 201.

[213] "Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan,

Conspiracy to violate section 793 is likewise punishable by imprisonment for not more than 10 years (not more than 20 years for a subsequent offense) and/or a fine of not more than $250,000, 18 U.S.C. 793(g), and criminal forfeiture of any proceeds derived from the offense, 18 U.S.C. 793(h).

Section 794 essentially subjects transgressions similar to those banned in section 793 to more severe penalties if they involve gathering national defense information for a foreign nation or to injure the United States,[214] particularly if the offense is committed in war time.[215] Conspirators are subject to the same penalties, 18 U.S.C. 794(c), and property derived from a violation or used to facilitate a violation is subject to forfeiture.[216]

---

map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer . . . Shall be fined under this title or imprisoned not more than ten years, or both," 18 U.S.C. 793(f).

[214] "Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or, if there is no jury, the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy," 18 U.S.C. 794(a).

[215] "Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life," 18 U.S.C. 794(b).

[216] "(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law – (A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation, and (B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation. For the purposes of this

Section 798 protects military and diplomatic codes and government codebreaking. It proscribes unlawful dissemination of classified information concerning communications intelligence and government cryptography.[217] Violations

---

subsection, the term 'State' includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

"(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

"(3) The provisions of subsections (b), (c) and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)-(p)) shall apply to – (A) property subject to forfeiture under this subsection; (B) any seizure or disposition of such property; and (C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

"(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law," 18 U.S.C. 794(d).

[217] "(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information – (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or (3) concerning the communication intelligence activities of the United States or any foreign government; or (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes – Shall be fined under this title or imprisoned not more than ten years, or both.

"(b) As used in subsection (a) of this section -- The term 'classified information' means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution; The terms 'code,' 'cipher,' and 'cryptographic system' include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications; The term `foreign government' includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States; The term 'communication intelligence' means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients; The term 'unauthorized person' means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

"(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof."

are punishable by imprisonment for not more than 10 years and/or a fine of not more than $250,000, 18 U.S.C. 798(a), 3571, and the confiscation of any property derived from the offense or used to facilitate its commission, 18 U.S.C. 798(d).[218]

RICO and money laundering.

Violations of section 793, 794, 798 or 1030 are money laundering predicate offenses, 18 U.S.C. 1956(c)(7)(D), and thereby also become RICO predicates, 18 U.S.C. 1961. Moreover, violations of paragraph 1030(a)(1) are among the offenses listed in 18 U.S.C. 2332b(g)(5)(B) (federal crimes of terrorism) and are consequently RICO predicate offenses, 18 U.S.C. 1961(1)(G).

APPENDIX

Selected Bibliography

Articles

Friendman & Bissinger, *"Infojacking": Crimes on the Information Super Highway*, 9 JOURNAL OF PROPERTY RIGHTS 2 (1997)

Heymann, *Legislating Computer Crime*, 34 HARVARD JOURNAL ON LEGISLATION 373 (1997)

Kerr, *Search and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE (July, 2002), on www.cybercrime.gov (Nov.21, 2003)

Levinson & Paetsch, *The Computer Fraud and Abuse Act: A Powerful New Way to Protect Information,* 19 COMPUTER & INTERNET LAWYERS 11 (Sept. 2002)

Olivenbaum, *<CTRL><ALT><DELETE>: Rethinking Federal Computer Crime Legislation,* 27 SETON HALL LAW REVIEW 574 (1997)

---

[218] "(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law – (A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and (B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation. (2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1). (3) Except as provided in paragraph (4), the provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)-(p)), shall apply to – (A) property subject to forfeiture under this subsection; (B) any seizure or disposition of such property; and (C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection. (4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law. (5) As used in this subsection, the term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States," 18 U.S.C. 798(d).

Sinrod & Reilly, *Cyber-Crime: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECHNOLOGY LAW JOURNAL 177 (2000)

Soma, Banker & Smith, *Computer Crime: Substantive Statutes and Technical and Legal Search Considerations*, 39 AIR FORCE LAW REVIEW 225 (1996)

Notes

Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet, 12 SANTA CLARA COMPUTER & HIGH TECHNOLOGY LAW JOURNAL 403 (1996)

The Limits of Computer Conversion: United States v. Collins, 9 HARVARD JOURNAL OF LAW & TECHNOLOGY 205 (1996)

Nineteenth Survey of White Collar Crime: Computer Crimes, 41 AMERICAN CRIMINAL LAW REVIEW 285 (2004)

18 U.S.C. 1030

(a) 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;
(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;
(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;
(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;

(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 subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--
(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
(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;
(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.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is–
(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if–
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was 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
(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(4)(A) a fine under this title except as provided in paragraph (5), imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
(B) a fine under this title except as provided in paragraph (5), imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
(C) a fine under this title except as provided in paragraph (5), imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
(5)(A) If the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
(B) If the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.
(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section–
(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(2) the term "protected computer" means a computer–
(A) 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
(B) which is 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;
(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term "financial institution" means–
(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;
(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means 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;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means 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; and
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

http://www.crsdocuments.com