

Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws

Charles Doyle
Senior Specialist in American Public Law

March 21, 2012

Congressional Research Service
7-5700
www.crs.gov
RS20830

CRS Report for Congress
Prepared for Members and Committees of Congress
c11173008

Summary

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, outlaws conduct that victimizes computer systems. It is a cyber security law. It protects federal computers, bank computers, and computers connected to the Internet. 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 cracks and gaps in the protection afforded by other federal criminal laws. This is a brief sketch of CFAA and some of its federal statutory companions, including the amendments found in the Identity Theft Enforcement and Restitution Act, P.L. 110-326, 122 Stat. 3560 (2008).

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., hacking) resulting in exposure to certain governmental, credit, financial, or computer-housed information, 18 U.S.C. 1030(a)(2);
- damaging a government computer, a bank computer, or a computer used in, or affecting, 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, or affecting, 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, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(7);
- trafficking in passwords for a government computer, or when the trafficking affects 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 or conspire 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 for victims of these crimes. Subsections 1030(i) and (j) authorize forfeiture of tainted property.

This report is an abridged version of CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle, stripped of the authorities and footnotes found there.

Contents

Introduction 1
Trespassing in Government Cyberspace (18 U.S.C. 1030(a)(3)) 1
Obtaining Information by Unauthorized Computer Access (18 U.S.C. 1030(a)(2)) 2
Causing Computer Damage (18 U.S.C. 1030(a)(5)) 2
Computer Fraud (18 U.S.C. 1030(a)(4)) 3
Extortionate Threats (18 U.S.C. 1030(a)(7)) 4
Trafficking in Computer Access (18 U.S.C. 1030(a)(6)) 5
Computer Espionage (18 U.S.C. 1030(a)(1)) 5

Contacts

Author Contact Information 6

Introduction

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, or affecting, 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, or affecting, 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, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(7);
- trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce, 18 U.S.C. 1030(a)(6);
- accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1)

Subsection 1030(b) makes it a crime to attempt or conspire 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 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. Subsection 1030(h) calls 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)). Subsections 1030(i) and (j) authorize the confiscation of property generated by, or used to facilitate the commission of, one of the offenses under subsection 1030(a) or (b).

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

Paragraph 1030(a)(3) condemns unauthorized intrusion ("hacking") into federal government computers whether they are used exclusively by the government or the federal government shares access with others. Broken down into its elements, paragraph (a)(3) makes it unlawful for anyone who

- without authorization
- intentionally
- either
  - accesses a government computer maintained exclusively for the use of the federal government, or

- accesses 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.

Consequences: Imprisonment for not more than one year (not more than 10 years for repeat offenders) and/or a fine under Title 18 (the higher of $100,000 for misdemeanors/$250,000 for felonies or twice the amount of the loss or gain associated with the offense, 18 U.S.C. 3571). These, like most federal offenses committed by juveniles, are usually tried in state court. Violations of each of the paragraphs of subsection 1030(a) may trigger forfeiture, restitution, money laundering, civil liability and racketeering provisions found elsewhere.

Other criminal liability: attempt, conspiracy, complicity & more: An attempt to violate any of the paragraphs of subsection 1030(a), and conspiracy to violate any federal law are separate federal crimes, 18 U.S.C. 1030(b), 371.

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. It may 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.

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

One step beyond simple hacking is the prohibition against acquiring certain protected information by intentional unauthorized access. It covers three types of information—information of the federal government, consumer credit or other kinds of financial information, and information acquired from a protected computer.

Penalties: Simple violations: not more than one year and/or a fine under Title 18, 18 U.S.C. 1030(c)(2)(A); violations for gain or involving more than $5,000: not more than five years and/or a fine under Title 18; repeat offenders: not more than 10 years and/or a fine under Title 18, 18 U.S.C. 1030(c). Offenders are also subject to civil liability, 18 U.S.C. 1030(g).

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.

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

Paragraph 1030(a)(5) proscribes unleashing worms or viruses or otherwise causing computer damage, that is, (A) intentionally causing unauthorized damage by knowingly causing a transmission to a protected computer; (B) recklessly causing damage by intentionally accessing a protected computer; or (C) causing damage and loss by intentionally accessing a protected computer. 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 (1) used exclusively for or by the United States Government; (2) used

exclusively for or by a bank or other financial institution; (3) used in part for or by the United States Government where the damage "affects" government use or use on the government's behalf; (4) 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 (5) used in, or affecting, interstate or foreign commerce or communications.

Penalties: Recidivism and causing serious damage recklessly or intentionally are punished more severely than first offenses or causing damage without necessarily intending to do so or than causing less serious damage intentionally or recklessly. First-time offenders that do not cause serious damage are punishable by imprisonment of not more than one year. When an offender with a prior conviction causes damage that is not serious, he is punishable by imprisonment for more than 10 years. Offenders with a prior conviction who intentionally or recklessly cause damage that is not serious are punishable by imprisonment for not more than 20 years.

On the other hand, intentionally causing serious 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). Recklessly causing serious damage following unauthorized access or attempted access carries a penalty of imprisonment for not more than five years (not more than 20 years for a second or subsequent offense). 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 20 years (any term of years or life if death results).

Other than physical injury or death, the types of serious damage that trigger more severe punishment are damage that (1) causes a loss that over the course a year exceeds $5,000; (2) modifies, impairs, or could modify or impair medical services; (3) causes physical injury; (4) threatens public health or safety; (5) affects a justice, national defense, or national security entity computer; or (6) affects 10 or more protected computers over the course of a year.

Other Crimes: The general observations concerning attempt, conspiracy and complicity noted for the simple trespass paragraph apply here. In addition, 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. A partial inventory might include 18 U.S.C. 844(f)(destruction of federal property by arson or explosion); 18 U.S.C. 1853 (destruction of timber of U.S. lands); 18 U.S.C. 2071 (destruction of government records); 18 U.S.C. 1361 (destruction of federal property); 18 U.S.C. 1362 (destruction of federal communications property); 18 U.S.C. 32 (destruction of aircraft or aircraft facilities); 18 U.S.C. 33 (destruction of motor vehicles or their facilities); 18 U.S.C. 2280 (destruction of maritime navigational facilities); 18 U.S.C. 1992 (causing a train wreck); 18 U.S.C. 1367 (damaging an energy facility).

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

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).

Penalties: not more than five years (not more than 10 years for subsequent offenses) and/or a fine under Title 18, 18 U.S.C. 1030(c)(4). Victims may sue for compensatory damages and/or injunctive relief, 18 U.S.C. 1030(g).

Other Crimes: Earlier observations with respect to attempt, conspiracy and complicity apply with equal force here. Other federal laws that might be implicated are 18 U.S.C. 1343 (wire fraud); 18 U.S.C. 2314 (interstate transportation of stolen property); 18 U.S.C. 659 (theft from interstate carriers); 18 U.S.C. 1832 (economic espionage); 18 U.S.C. 1832 (theft of trade secrets); 18 U.S.C. 1029 (fraud involving credit cards and access devices); 18 U.S.C. 641 (theft of federal property); 18 U.S.C. 1001 (false statements on a matter within the jurisdiction of a federal agency or department); 18 U.S.C. 1014 (false statements on federally insured loan and credit applications); 18 U.S.C. 1010, 1012 (false statements concerning various HUD transactions); 18 U.S.C. 287 (false claims against the United States); 18 U.S.C. 1344 (bank fraud); 18 U.S.C. 657 (theft or embezzlement by officer or employee of lending, credit and insurance institutions); 18 U.S.C. 1005 (false entries bank officers or employees); 18 U.S.C. 1006 (false entries by officers or employees of federal credit institutions); 18 U.S.C. 1007 (false statements to influence the Federal Deposit Insurance Corporation); 18 U.S.C. 2319 (copyright infringement); 18 U.S.C. 1956 & 1957 (money laundering); 18 U.S.C. 1962 (racketeering); 18 U.S.C. 1952 (travel act).

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

This 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, that
  - causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals
  - modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals
  - causes physical injury to any person; or
  - threatens public health or safety" (1030(e)(8))]
- to a protected computer
- with the intent to extort money or a thing of value
- from any person, firm, association, educational institution, financial institution, government entity, or other legal entity.

Penalties: not more than five years (not more than 10 years for second and subsequent offenses) and/or a fine under Title 18, 18 U.S.C. 1030(c), and victims may claim the advantages of the civil cause of action available under 18 U.S.C. 1030(g).

Other crimes: The general observations concerning attempt, conspiracy and complicity noted with respect to the other paragraphs of 1030(a) apply here. Violations of paragraph 1030(a)(7)

may also offend 18 U.S.C. 1951 (extortion that affects commerce); 18 U.S.C. 875 (threats transmitted in interstate commerce); 18 U.S.C. 876 (mailing threatening communications); 18 U.S.C. 877 (mailing threatening communications form a foreign country); and 18 U.S.C. 880 (receipt of the proceeds of extortion).

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

Paragraph 1030(a)(6) outlaws misconduct similar to the access device proscriptions of Section 1029. Although limited, it provides several distinct advantages. First, it covers passwords to government computers more clearly than does Section 1029. Second, as something 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) of 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
- either
  - of a federal computer or
  - in a manner that affects interstate or foreign commerce.

Penalties: not more than one year (not more than 10 years for repeat offenders) and/or a fine under Title 18, 18 U.S.C. 1030(c)(2). Offenders are also civilly liable to their victims, 18 U.S.C 1030(g).

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) and the wire fraud provisions of 18 U.S.C. 1343. Nevertheless, either of these may provide the foundation for a RICO (18 U.S.C. 1962) or money laundering (18 U.S.C. 1956, 1957) prosecution, so that should conduct in violation of paragraph 1030(a)(6) also offend either the mail fraud or credit card fraud prohibitions, a criminal breach of RICO or the money laundering provisions may also have occurred.

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

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 U.S. national defense and well being, or more simply laws that outlaw spying. The distinctive feature of paragraph 1030(a)(1) is

its merger of elements of espionage and computer abuse. 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
- classified information concerning national defense, foreign relations or atomic energy
- with reason to believe that the information either
  - could be used to injure the United States, or
  - could be used to the advantage of a foreign nation
- when the information was acquired by unauthorized computer access.

Penalties: not more than 10 years (not more than 20 years for repeat offenders) and/or a fine under Title 18, 18 U.S.C. 1030(c)(1).

Other Crimes: Espionage prosecutions are not common. The attempt, conspiracy and complicity observations continue to apply and the RICO (18 U.S.C. 1962) and money laundering (18 U.S.C. 1956, 1957) may be implicated through the application of Sections 793, 794 or 798 to conduct that offends paragraph 1030(a)(1).

Author Contact Information

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968