

PROSECUTING COMPUTER CRIMES

Computer Crime and
Intellectual Property Section
Criminal Division

H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director,
OLE

Scott Eltringham
Computer Crime
and Intellectual
Property Section
Editor in Chief



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

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes, and makes no public release of it. Individuals receiving the book in training are reminded to treat it confidentially.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. See *United States v. Caceres*, 440 U.S. 741 (1979).

Appendix B

Jury Instructions

18 U.S.C. § 1030: Generally Applicable Definitions

For purposes of instruction[s] ____, the term[s]:

“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. (Source: 18 U.S.C. § 1030(e)(1))

“Damage” means any impairment to the integrity or availability of data, a program, a system, or information. (Source: 18 U.S.C. § 1030(e)(8))

“Department of the United States” means the legislative or judicial branch of the United States Government or one of the executive departments. (Source: 18 U.S.C. § 1030(e)(7))

“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. (Source: 18 U.S.C. § 1030(e)(6))

“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. (Source: 18 U.S.C. § 1030(e)(9))

“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. (Source: 18 U.S.C. § 1030(e)(11))

“Person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity. (Source: 18 U.S.C. § 1030(e)(12))

“Protected computer” means a computer

- [exclusively for the use of *[a financial institution][the United States Government]*]
- [used *[by][for] [a financial institution][the United States Government]* and the conduct constituting the offense affects that use *[by][for] [the financial institution][the United States Government]*]
- [which is *[used in][affecting] [interstate][foreign] [commerce][communication]*, including a computer located outside the United States that is used in a manner that affects *[interstate][foreign] [commerce][communication]* of the United States].

(Source: 18 U.S.C. § 1030(e)(2))

18 U.S.C. § 1030(a)(1)

Computer Fraud—Obtaining National Security Information

The crime of accessing a computer to obtain national security information, as charged in [Count ____] of the indictment, has four essential elements, which are:

One, the defendant[s] knowingly accessed a computer [*without authorization*][*exceeding authorized access*];

Two, the defendant[s] obtained information that

- [has been determined by the United States government by [*Executive Order*][*statute*] to require protection against unauthorized disclosure for reasons of [*national defense*][*foreign relations*]
- [restricted data regarding the design, manufacture or use of atomic weapons];

Three, the defendant[s] had reason to believe that the information obtained could be used to the injury of the United States or to the advantage of any foreign nation; and

Four, the defendant[s] voluntarily and intentionally¹

- [[*caused to be*] [*communicated*][*delivered*][*transmitted*] the information to a person not entitled to receive it]
- [retained the information and failed to deliver the information to an officer or employee of the United States entitled to receive the information].

The government is not required to prove that the information obtained by the defendant[s] was in fact used to the injury of the United States or to the advantage of any foreign nation.

Specific definitions

The phrase “restricted data” means all data concerning the: (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, not declassified or removed pursuant to federal law. (Source: 42 U.S.C. § 2014(y))

¹ The statute uses the term “willfully,” but consistent with Committee Comments to Instruction 7.02, that term has been replaced with the words “voluntarily and intentionally.”

18 U.S.C. § 1030(a)(2)

Computer Fraud—Obtaining Confidential Information

The crime of computer fraud to obtain confidential information, as charged in [Count ____] of the indictment, has *[two][three]* essential elements, which are:

One, the defendant[s] intentionally accessed a computer *[without authorization][exceeding authorized access]*;

Two, the defendant[s] obtained information

- *[contained in a financial record of [a financial institution][an issuer of a credit card]]*
- *[on a consumer contained in a file of a consumer reporting agency]*
- *[from any [department][agency] of the United States]*
- *[from any protected computer];*

[Three, the defendant[s]²

- *[acted for purposes of commercial advantage or private financial gain]*
- *[acted in furtherance of (describe criminal or tortious act)]*
- *[obtained information having a value exceeding \$5,000.00]].*

Specific Definitions

The phrase “consumer reporting agency” means any person or entity 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 for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of

² In most felony cases charged under 18 U.S.C. § 1030(a)(2), element three should be submitted to the jury because these facts would increase the statutory maximum penalties. See 18 U.S.C. §§ 1030(c)(2)(B). Any fact (other than a prior conviction) that increases the maximum penalty for a crime must be charged in the indictment, submitted to the jury, and proven beyond a reasonable doubt. *Apprendi v. New Jersey*, 530 U.S. 466 (2000). These aggravating factors can be submitted as a formal element or by special interrogatory. Note that element three should not be submitted if the government has charged a first time offender of section 1030 solely with a misdemeanor, see 18 U.S.C. § 1030(c)(2)(A), or if it has charged a felony offense that allegedly occurred after a conviction for another offense under section 1030. See 18 U.S.C. § 1030(c)(2)(C). Finally, if requested by a party and if supported by the evidence, the court can submit a “greater and lesser included offense” instruction that would permit separate findings on the aggravating elements as well as a charge without such findings (i.e., a misdemeanor).

interstate commerce for the purpose of preparing or furnishing consumer reports. (Source: 18 U.S.C. § 1030(a)(2)(A); *see also* 15 U.S.C. § 1681 et seq.)

The phrase “financial institution” means:

- [an institution with deposits insured by Federal Deposit Insurance Corporation]
- [the Federal Reserve or a member of the Federal Reserve, including any Federal Reserve Bank]
- [a credit union with accounts insured by the National Credit Union Administration]
- [a member of the Federal home loan bank system and any home loan bank]
- [any institution of the Farm Credit System]
- [a broker-dealer registered with the Securities and Exchange Commission]
- [the Securities Investor Protection Corporation][a branch or agency of a foreign bank]
- [a national banking association or corporation lawfully engaged in international or foreign banking].

(Source: 18 U.S.C. § 1030(e)(4))

The phrase “financial record” means information derived from any record held by [*a financial institution*][*an issuer of a credit card*] pertaining to a customer’s relationship with that entity. (Source: 18 U.S.C. § 1030(e)(5)).

If desired, the Court may instruct the jury that the phrase “obtained information” “includes merely reading the information. There is no requirement that the information be copied or transported.” S. Rep. 104-357, at 7 (1996), *available at* 1996 WL 492169. In earlier amendments addressing other subsections of section 1030, Congress has also stated that the phrase “obtained information” includes the mere observation of the data and does not require the government to prove the data was removed from its original location or transcribed. *See* S. Rep. No. 99-432, at 6-7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 *and available at* 1986 WL 31918. The term “information” includes information stored in intangible form. *See* S. Rep. No. 357, 104th Cong., 2d Sess. 8 (1996).

18 U.S.C. § 1030(a)(3)

Computer Fraud—Accessing a Nonpublic Computer

The crime of accessing a nonpublic computer, as charged in [Count ____] of the indictment, has three essential elements, which are:

One, the defendant[s] intentionally accessed a nonpublic computer of a[n] *[department]**[agency]* of the United States;

Two, the defendant[s] were without authorization to access any nonpublic computer of that *[department]**[agency]*; and

Three, the defendant[s] accessed a nonpublic computer that was

- [exclusively for the use of the United States Government]
- [used *[by]**[for]* the United States Government, and the defendant[s]'s conduct affected that use *[by]**[for]* the United States Government].

18 U.S.C. § 1030(a)(4)

Computer Fraud—Accessing a Computer to Defraud and Obtain Value

The crime of accessing a computer to defraud and obtain value, as charged in [Count ____] of the indictment, has three essential elements, which are:

One, the defendant[s] knowingly and with intent to defraud accessed a protected computer *[without authorization][exceeding authorized access]*;

Two, the defendant[s], by accessing the protected computer *[without authorization][exceeding authorized access]*, furthered the intended fraud; and

Three,

- [the defendant[s] thereby obtained anything of value]
- [the object of the fraud was the use of the computer and the value of such use exceeded \$5,000 in any one year.]

18 U.S.C. § 1030(a)(5)(A)

Computer Fraud—Transmission Of Program To Cause Damage To A Computer

The crime of transmission of a program to cause damage to a computer, as charged in [Count ____] of the indictment, has *[two][three]* essential elements, which are:

One, the defendant[s] knowingly caused the transmission of *[a program][information][code][a command]* to a protected computer; and

Two, the defendant[s], as a result of such conduct, intentionally caused damage to a protected computer without authorization; and

[Three, as a result of such conduct, the defendant[s] caused:

- [loss to one or more persons during any one year period of an aggregate value of \$5,000.00 or more]
- [loss resulting from a related course of conduct affecting one or more other protected computers of an aggregate value of \$5,000.00 or more]
- [the *[potential]* modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals]
- [physical injury to any person]
- [a threat to public health or safety]
- [damage affecting a computer used *[by][for]* a government entity (describe entity at issue), in furtherance of the administration of justice, national defense, or national security]
- [damage affecting ten or more protected computers during any one year period]]³

³ In most felony cases charged under 18 U.S.C. § 1030(a)(5)(A), element three, modified to conform to the allegations in the indictment, should be submitted to the jury because these facts would increase the statutory maximum penalties. See 18 U.S.C. §§ 1030(c)(4)(B), (E) & (F); *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Note that element three should not be submitted if the government has charged a misdemeanor or if it has charged a felony offense that allegedly occurred after a conviction for another offense under section 1030. If requested by a party and if supported by the evidence, the court can submit a “greater and lesser included offense” instruction that would permit separate findings on the aggravating elements as well as a charge without such findings (i.e., a misdemeanor).

[Three, as a result of such conduct, the defendant[s] [*attempted to cause*][*knowingly caused*][*recklessly caused*] [*serious bodily injury*][*death*]]⁴

⁴ The second alternative element three addresses greater aggravating elements set forth in 18 U.S.C. §§ 1030(c)(4)(E)&(F). If the evidence also supports any one of the lesser aggravating elements from the first alternative element three, the court can submit a “greater and lesser included offense” instruction that would permit separate findings on both the lesser and the greater aggravating elements.

18 U.S.C. § 1030(a)(5)(B)&(C)

Computer Fraud—Causing Damage To a Computer

The crime of causing damage to a computer or information, as charged in [Count ____] of the indictment, has *[two][three]* essential elements, which are:

One, the defendant[s] intentionally accessed a protected computer without authorization; and

Two, the defendant[s], as a result of such conduct, *[recklessly caused damage][caused damage and loss]*;

[Three, as a result of such conduct, the defendant[s] caused:

- [loss to one or more persons during any one year period of an aggregate value of \$5,000.00 or more]
- [loss resulting from a related course of conduct affecting one or more other protected computers of an aggregate value of \$5,000.00 or more]
- [the *[potential]* modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals]
- [physical injury to any person]
- [a threat to public health or safety]
- [damage affecting a computer used *[by][for]* a government entity (describe entity at issue), in furtherance of the administration of justice, national defense, or national security]
- [damage affecting ten or more protected computers during any one year period]].⁵

⁵ In most felony cases charged under 18 U.S.C. § 1030(a)(5)(A), element three, modified to conform to the allegations in the indictment, should be submitted to the jury because these facts would increase the statutory maximum penalties. See 18 U.S.C. §§ 1030(c)(4)(B), (E) & (F); *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Note that element three should not be submitted if the government has charged a misdemeanor or if it has charged a felony offense that allegedly occurred after a conviction for another offense under section 1030. If requested by a party and if supported by the evidence, the court can submit a “greater and lesser included offense” instruction that would permit separate findings on the aggravating elements as well as a charge without such findings (i.e., a misdemeanor).

18 U.S.C. § 1030(a)(6)

Computer Fraud—Trafficking in Passwords

The crime of trafficking in passwords, as charged in [Count ____] of the indictment, has three essential elements, which are:

One, the defendant[s] knowingly

- [transferred to another person any password or similar information through which a computer may be accessed without authorization]
- [obtained control of any password or similar information through which a computer may be accessed without authorization, with the intent to transfer it to another person]⁶;

Two, the defendant[s] acted with the intent to defraud; and

Three,

- [the defendant[s]’s act[s] affected *[interstate][foreign]* commerce]
- [the computer was used *[by][for]* the United States government].

⁶ Element one incorporates the definition of “traffic” found in 18 U.S.C. § 1030(a)(6) through its cross reference to 18 U.S.C. § 1029(e)(5). In addition to using the term “transfer,” the definition of traffic from section 1029(e)(5) includes the phrase “dispose of,” not included in this instruction.

18 U.S.C. § 1030(a)(7)

Computer Fraud—Threatening to Damage a Protected Computer or Information

The crime of threatening to damage a protected computer, as charged in [Count ____] of the indictment, has three essential elements, which are:

One, the defendant[s] transmitted any communication in [*interstate*][*foreign*] commerce;

Two, the defendant[s] transmitted the communication with the intent to extort any [*money*][*thing of value*] from any person; and

Three, the communication contained any

- [threat to cause damage to a protected computer]
- [threat to obtain information from a protected computer [*without authorization*][*exceeding authorized access*]]
- [threat to impair the confidentiality of information obtained from a protected computer [*without authorization*][*exceeding authorized access*]]
- [*demand*][*request*] for [*money*][*thing of value*] in relation to damage to a protected computer, and the defendant[s] caused the damage to facilitate the extortion of the [*money*][*thing of value*].

Specific Definitions

The phrase “intent to extort” means an intent to obtain the property of another with his or her consent by the wrongful use of actual or threatened force, violence or fear or under color of official right. (Source: 18 U.S.C. § 1951(b)(2))