Congressional Research Service
Informing the legislative debate since 1914

Cyber Crime: Conduct and Related Computer Fraud and Abuse (CFAA) Act in the 116th Cong

September 21, 2020

Congressional Research Service
https://crsreports.congress.gov
R46536

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMAR

R46536

September 21, 2020

Peter G. Berris
Legislative Attorney

Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is a civil and criminal cybercrime law prohibiting a variety of computer-related conduct. Although sometimes described as an anti-hacking law, the CFAA is much broader in scope. Indeed, it prohibits seven categories of conduct including, with certain exceptions and conditions:

1. Obtaining national security information through unauthorized computer access and sharing or retaining it;
2. Obtaining certain types of information through unauthorized computer access;
3. Trespassing in a government computer;
4. Engaging in computer-based frauds through unauthorized computer access;
5. Knowingly causing damage to certain computers by transmission of a program, information, code, or command;
6. Trafficking in passwords or other means of unauthorized access to a computer;
7. Making extortionate threats to harm a computer or based on information obtained through unauthorized access to a computer.

Since the original enactment of the CFAA in 1984, technology and the human relationship to it have continued to evolve. Although Congress has amended the CFAA on numerous occasions to respond to new conditions, the rapid pace of technological advancement continues to present novel legal issues under the statute. For example, with increasing computerization has come a corresponding proliferation of Terms of Service (ToS) agreements — contractual restrictions on computer use. But federal courts disagree on whether the CFAA imposes criminal liability for ToS violations, and the United States Supreme Court is currently considering a case on this issue. Another technological development that has created tension under the CFAA is the rise of botnets, which are networks of compromised computers often used by cybercriminals. Although the CFAA prohibits creating botnets and using them to commit certain crimes, it is unclear if selling or renting a botnet violates the statute — a potential concern given that botnet access is often rented from botnet brokers. On a more basic level, another change that has prompted some reexamination of the CFAA is the seemingly-growing frequency of computer crime. Some contend that the prevalence and perniciousness of hacking requires private actors to defend themselves by hacking back — that is, initiating some level of intrusion into the computer of the initial attacker. The same provisions of the CFAA that prohibit hacking ostensibly also make it a crime to hack back, which some legislation has sought to change.

Contents

.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Tables

.....
.....
.....
.....

Contacts

.....

Introduction

1

2 3

4

5

6

7

8

[1] According to the United States Census Bureau (Census Bureau), by one measure only 8% of households had a computer in 1984. CAMILLE RYAN & JAMIE M. LEWIS, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2015, U.S. CENSUS BUREAU 2 (Sept. 2017), https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-37.pdf. That same report indicated that the percentage increased to 87% of households in 2015, up from 84% in 2013. *Id.* For its part, the Federal Trade Commission has estimated that 50 billion devices will be connected to the Internet of Things (IoT) in 2020, a figure that includes internet-enabled devices such as smart appliances and fitness trackers. FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD i (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. For a review of Computer Fraud and Abuse Act (CFAA) issues unique to the IoT, see generally Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 162 (Feb. 14, 2018). As discussed below, these devices are computers in the context of the CFAA. *See infra* Computer

[2] United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015).

[3]
regarding internet-enabled crimes 300 every day. FBI, *2019 Internet Crime Report Released* (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120. The actual number of computer and internet crimes is almost certainly higher, as many may escape detection entirely. *See* Beale, *supra* note 1, at 167
compromised . . . [as] [m]any objects connected to the internet continue to serve the function for which consumers purchased them long aft *see also* Michel Cukier, *Study: Hackers Attack Every 39 Seconds*, A. JAMES CLARK SCH. OF ENG G (Feb. 9, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds#:~:text=A%20Clark%20School%20study%20is,attackers%20more%20chance%20of%20success (concluding that computers connected to the internet are attacked

[4] Philip Ewing, *Twitter Attack Underscores Broad Cyber Risks Still Facing U.S. Elections*, NPR (July 17, 2020), https://www.npr.org/2020/07/17/892044086/twitter-attack-underscores-broad-cyber-risks-still-facing-u-s-elections.

[5] Chris Fox & Leo Kelion, *Coronavirus: Russian Spies Target Covid-19 Vaccine Research*, BBC (July 16, 2020), https://www.bbc.com/news/technology-53429506.

[6] CRS Legal Sidebar LSB10446, *An Overview of Federal Criminal Laws Implicated by the COVID-19 Pandemic*, by Peter G. Berris.

[7] This Report cites to
nterpretations of federal statutes
ORIN S. KERR, COMPUTER CRIME
LAW 31, 75 (3d ed. 2013).

[8] H.R. REP. NO. 98-894, at 10 (1984) (with the capability of the personal

9

10

11

-

12

13

14

15

16

History of the CFAA

WarGames[17]

[18] WarGames

[9] For example, relevant provisions might include, among others, federal laws criminalizing wire fraud under 18 U.S.C. § 1343, cyberstalking under 18 U.S.C. § 2261A, the interception of electronic communications under 18 U.S.C. § 2511, or the unlawful access of stored communications under 18 U.S.C. § 2701. For an examination of how these and other statutes apply to cybercrime, see generally U.S. DEP T OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, PROSECUTING COMPUTER CRIMES (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[10] DANIEL ETCOVICH & THYLA VAN DER MERWE, COMING IN FROM THE COLD: A SAFE HARBOR FROM THE CFAA AND THE DMCA § 1201 FOR SECURITY RESEARCHERS, BERKMAN KLEIN CTR. RSCH. PUBL N NO. 2018-4, HARVARD UNIV. 7 (2018), https://dash.harvard.edu/bitstream/handle/1/37135306/ComingOutoftheCold_FINAL.pdf#page=11.

[11] 18 U.S.C. § 1030.

[12] *See* U.S. DEP T OF JUSTICE, *supra* note 9, at 35 (providing examples of the types of conduct that may be prosecuted

[13] *See, e.g.*, Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 479, 481 (2019) O]ur definitive computer intrusion statute, the [CFAA], belies its last-century crafting, as it strains under the new threat vectors leveraged by this century s formidable *Reevaluating the Computer Fraud and Abuse Act: Amending the Statute to Explicitly Address the Cloud*, 86 FORDHAM L. REV. 767, 770 (2017) in practice [the CFAA] has not been able to keep up with and examining whether the law adequately protects computers connected to the cloud); Marcelo Triana, *Is Selling Malware A Federal Crime?*, 93 N.Y.U. L. REV. 1311, 1315 (2018) (examining whether the CFAA prohibits the sale of malware).

[14] *See generally* CRS Legal Sidebar LSB10423, *From Clickwrap to RAP Sheet: Criminal Liability under the Computer Fraud and Abuse Act for Terms of Service Violations*, by Peter G. Berris (examining judicial disagreement on the breadth of the CFAA with respect to Terms of Service Agreements violations).

[15] *See infra* Botnet Trafficking

[16] *See infra* Hacking Back

[17] WARGAMES (Metro-Goldwyn-Mayer Studios 1983).

[18] *See* Fred Kaplan, ‘ W a r G a m e s ’ a n d C y b e r s e c u r i t y *Hack*, N.Y. TIMES (Feb. 19, 2016), o a H o l l y w o

19

20

21

22

23

24

25

26

27

28

29

https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html

et al., *Is Tricking A Robot Hacking?*, 34 BERKELEY TECH. L.J. 891, 904 (2019)
agan saw the movie *War Games* and met with his national security advisers
Jay
P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 492 (2012)

[19] *See* Roger Ebert, *WarGames*, ROGEREBERT.COM (June 3, 1983), https://www.rogerebert.com/reviews/wargames-1983 (reviewing and summarizing plot of *WarGames*).

[20] H.R. REP. NO. 98-894, at 10 (1984) (referencing *WarGames* in discussion of necessity of computer fraud legislation).

[21] Kaplan, *supra* note 18.

[22] Evtimov, *supra* note 18, at 904.

[23] *See* CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle, at n.2 (chronicling legislative history of CFAA).

[24] Greg Pollaro, Note, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12, 4 (Aug. 26, 2010).

[25] Pub. L. No. 98-473, § 2102, 98 Stat. 1837 (1984) (codified at 18 U.S.C. § 1030).

[26] *See, e.g.*, Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J.

[27] *See generally* S. REP. NO. 99-432, at 6 9 (1986) (summarizing concerns expressed by DOJ).

[28] Adams, *supra* note 26, at 422.

[29] *Id.* at 423.

[30]
[31] [32] [33]

Overview of the CFAA

Key CFAA Terms

[34]
[35]
[36]
[37]

Computer

[38] electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, any data storage facility or communications facility directly related to or operating in conjunction with such devic [39] The CFAA excludes only automated typewriters, typesetters, portable hand held calculators, and similar devices from its definition of computer.[40]

definition of computer is.[41] As one court explained, the definition includes any device with an electronic data processor, of which there are numerous examples.[42] Thus, under the CFAA, computers include not only laptops and desktops, but also a wide array of computerized

[30] *See* Doyle, *supra* note 23, at n.2 (listing CFAA amendments).

[31] *See* U.S. DEP T OF JUSTICE, *supra* note 9, at 1 2 (summarizing amendments to CFAA).

[32] The CFAA exists against the backdrop of numerous state computer crime laws that are beyond the scope of this Report. *E.g.*, VT. STAT. ANN. tit. 13, §§ 4101 07. Computer misuse statutes have been enacted KERR, *supra* note 7, at 29; *accord Computer Crime Statutes*, NAT L CONF. OF STATE LEGISLATURES (Feb. 24, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (conducting survey of the computer crime laws of all 50 states).

[33] *See* Evtimov, *supra* note 18, at 904 Since its implementation, the CFAA -

[34] *See id.*

[35] *See*

[36] *Id.*

[37] *See, e.g.*, *id.* in excess of authorization, and obtaining certain types of information).

[38] *See* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) (discussing breadth of CFAA with respect to the types of computers it governs).

[39] 18 U.S.C. § 1030(e)(1).

[40] *Id.*

[41] *Mitra*, 405 F.3d at 495 (emphasis omitted).

[42] United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

devices ranging from cellphones to objects embedded with microchips, such as certain microwave ovens, watches, and televisions.[43]

Protected Computers

Several provisions within the CFAA specifically concern [44] Among other things, the CFAA defines protec

used in or affecting interstate or foreign commerce or communication . . . . [45] Courts have construed the latter phrase as including any computer connected to the internet.[46] Thus, most modern computing devices are , including Internet of Things devices such as smart appliances and fitness trackers.[47] Another important type of computer that fits within the definition of protected computer is a server a computer that manage website data and other information.[48] For example, courts have concluded that the web servers storing and sharing the member data of a large social media website qualified as protected computers.[49]

---

[43] *Id.* at 902 03; *accord* United States v. Nosal, 844 F.3d 1024, 1050 (9th Cir. 2016) This means that nearly all desktops, laptops, servers, smart- box, Blu Ray player or any other Internet- (quoting United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012)); Berris, *supra* note **Error! Bookmark not defined.**, at 2 (describing CFAA anti-hacking law covering most computers, including laptops, desktops, websites, and computerized de

[44] 18 U.S.C. § 1030.

[45] *Id.* § 1030(e)(2).

[46] *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019)

effectively any computer connected to the Internet . . . including servers, computers that manage network resources and (quoting 18 U.S.C. § 1030(e)(2)(B)) (internal citations omitted)).

[47]

scarce, the general consensus among observers is that internet-enabled objects qualify as protected computers. *E.g.*, Beale, *supra* note 1, at 170; *accord* Matthew Ashton, Note, *Debugging the Real World: Robust Criminal Prosecution in the Internet of Things*, 59 ARIZ. L. REV. Phones, tablets, Fitbits, and even public transit cards with embedded computer chips are all included in the definition of a *protected computer* TJ Wong, *Is My Toaster a Computer? The Computer Fraud and Abuse Act and the Internet of Things*, COLUMB. J.L. & SOC. PROBS. (Mar. 30, 2019), http://jlsp.law.columbia.edu/2019/03/30/is-my-toaster-a-computer-the-computer-fraud-and-abuse-acts-definition-of-protected-computer-in-the-age-of-the-internet-of-things/ (explaining that the definition of computer includes ces feeding us data online, such as fitness watches and).

One interesting example from case law is that of *United States v. Peterson*. 776 F. App x 533 (9th Cir. 2019). In *Peterson*, the Federal Court of Appeals for the Ninth Circuit considered a vagueness challenge to a condition of supervised release imposed on a defendant convicted of possessing child pornography. *Id.* at 533. The condition at issue restricted the defendant from accessing a computer as defined by the CFAA. *Id.* at 534. In agreeing with the defendant that the condition was potentially overbroad, the court observed that a wide range of objects fall within the definition of computer unde Fitbit certain automobiles. *Id.* at n.3. Although the court did not discuss these devices in relation to protected

the court noted, Internet of Things devices are (1) computers (2) connected to the internet. *Id.*

[48] *hiQ Labs, Inc.*, 938 F.3d at 999.

[49] *Id.*

Without Authorization and Exceeds Authorized

50

51 52

53

54

with authorization

55

56

57

58

59

60

61

62

50 18 U.S.C. § 1030.

51 *Id*. § 1030(a)(2).

52 *Id*. § 1030.

53 *Id.*

54 *Id*. § 1030(e).

55 *Id*. (emphasis added).

56 *Id*. § 1030.

57 *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (explaining that employee was authorized by employer to use database).

58 hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1002 (9th Cir. 2019) (examining authority to access information on website servers as byproduct of that information being generally available to the public).

59 *See, e.g.*, *Rodriguez*, 628 F.3d at 1

;

Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) (describing how authorization was removed by a written cease and desist letter).

60 *See, e.g.*, *hiQ Labs, Inc.*, 938 F.3d at 1003 (exploring limits of authority based on whether use of a computer fell into category as a result of a cease and desist letter).

61

violations of contracts restricting the permissible uses of a given computer, such as employer computer use policies or ToS agreements contracts that govern the use of a product such as a website. *See infra* The CFAA and ToS Violations

62 *See infra* The CFAA and ToS Violations

authorized computer use, including: (1) code based restrictions such as passwords or other means of programming

63

64

65

66

67

68

declined to
69

Whatever the legislative intent, judicial interpretations
not been entirely consistent, and as one court opined, the difference
70

71

72

73

74

hardware or software to restrict access; (2) contractual restrictions such as Terms of Service agreements; and (3) social norms of computer use. KERR, *supra* note 7, at 40 41.

63 *See* U.S. DEP TOF JUSTICE, *supra* note 9, at 5 6 (recounting legislative history regarding intended meanings of

64 S. REP. No. 104-357, at 9 (1996) (describing outsiders as tho who gain access to a computer without authorization.

65 S. REP. No. 99-432, at 8 (1986).

66 *See* S. REP. No. 104-

67 S. REP. No. 99- who, while authorized to

68 *Id.* at 7.

69 *Id.*

70 LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006). According to Professor Orin S. Kerr, technological changes have blurred the line
Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner, Van Buren v. United States, No. 19-783, 2020 WL 4003433, at *16 (U.S. July 8, 2020).

71 *See, e.g.*, Rather, we hold that a person uses

employer has rescinded permission to access the comput

72 *See, e.g.*,

73 Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner, *supra* note 70, at *16.

74 *See* Int'l AiLLCport Ctrs.,

Prohibited Conduct under the CFAA

[75]

Cyber Espionage: 18 U.S.C. § 1030(a)(1)

[76]

[77]

[78]

[79]

[80]

[81]

[82]

terminated where he breached duty of loyalty and improperly erased em).

[75] The content of this section draws heavily from Doyle, *supra* note 23.

[76] 18 U.S.C. § 1030(a)(1) imposes criminal penalties on:

> (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.

[77] Doyle, *supra* note 23, at 71
prohibits the willful disclosure, attempted discl
are met).

[78] 18 U.S.C. § 1030(a)(1).

[79] U.S. DEP T OF JUSTICE, *supra* note 9, at 13.

[80] *See* KERR, *supra* note 7, at

[81] *See, e.g.*, Defense Department Linguist Charged with Espionage (Mar. 4, 2020), https://www.justice.gov/opa/pr/defense-department-linguist-charged-espionage (announcing charges against defendant under espionage statutes rather than § 1030(a)(1) for alleged conduct including improperly accessing United States

accord U.S. DEP T OF JUSTICE, *supra* note 9
1030(a)(1) and a federal espionage statute] . . . are applicable, prosecutors may tend towards using [the espionage statutes], for which guidance and prece

[82]

r S. REP. NO. 99-432,

83

84

85

86

87 by its own terms includes a range of activities including the failure to return national security information or the disclosure of that information. 88 89

Obtaining Information from a Protected Computer, 18 U.S.C. §1030(a)(2)

90

91

92

---

at 6 (1986) (quoting United States v. U.S. Gypsum Co., 438 U.S. 422, 445 (1978)). That description tracks judicial interpretations of the word knowing under other subsections of the CFAA, where courts have concluded that the term excludes accidental behavior. *See* QVC, Inc. v. Resultly, LLC, 99 F. Supp. 3d 525, 536 (E.D. Pa. 2015) (concluding

[83] 18 U.S.C. § 1030(a)(1).

[84] *Id.*

[85] *Id.*

[86] U.S. DEP T OF JUSTICE, *supra* note 9, at 14.

[87] 18 U.S.C. § 1030(a)(1).

[88] *Id.*

[89] *Id.*

[90] Section 1030(a)(2) imposes criminal liability on:

> (a) Whoever--
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer.

[91] *See* United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009)

(alterations in original) (quoting S. REP. NO. 99-432, at 6 7 (1986))); Am. Online, Inc. v.

preposition that § 1030(a)(2) covers not just theft but also the observation of data).

[92] *See Drew*, 259 F.R.D. at 457 n.13 (alteration in

93

94

95

96

intentional

97

98

99

100

101

Government Trespassing U.S.C. § 1030(a)(3)

102

103

104

original) (quoting S. REP. NO. 104 357, at 7 (1996))).

93 KERR, *supra* note 7, at 76.

94 United States v. Van Buren, 940 F.3d 1192, 1198 (11th Cir. 2019), *cert. granted*, No. 19-783, 2020 WL 1906566 (U.S. Apr. 20, 2020).

95 United States v. Gasperini, 894 F.3d 482, 487 (2d Cir. 2018).

96 *See generally* KERR, *supra* note 7, at 78 79 (explaining breadth of § 1030(a)(2) and why requirements in that

97 S. REP. NO. 99-432, at 5 (1986).

98 *Drew*

99 The provision also includes information obtained from card issuers and consumer reporting agencies. 18 U.S.C. § 1030(a)(2).

100 18 U.S.C. § 1030(a)(2).

101 *Drew*, 259 F.R.D. at 457.

102 18 U.S.C. § 1030(a)(3) imposes criminal liability on:

> (a) Whoever--
>
> (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

103 S. REP. NO. 99-

104 *E.g.*, Restatement (Second) of Torts § 158 (1965). Criminal liability for trespass under various statutes often

105

106

107

e x c l u s i v e l v 108

109

110

i n p a r t

111

112

113

114

115

116

117

refusal to vacate the area in which he is trespassing. *E.g.*, CONN. GEN. STAT. § 53a-107.

[105] Doyle, *supra* note 23
1030(a)(3).

[106] *See* U.S. DEP TOF JUSTICE, *supra* note 9, at 23, 25 (explaining why § 1030(a)(2) may in instances where both § 1030(a)(2) and § 1030(a)(3) could apply).

[107] 18 U.S.C. § 1030(a)(3).

[108] *Id.*

[109] *See* U.S. DEP TOF JUSTICE, *supra* note 9, at 24 (

[110] *Id.*

[111] 18 U.S.C. § 1030(a)(3).

[112] U.S. DEP TOF JUSTICE, *supra* note 9, at 24.

[113] *Id.*; *accord* Sawyer v
violation of 18 U.S.C. § 1030(a)(3) . . . do not include the requirement that the prohibited access to the computer system be for the specific purpose of defrauding the government. Rather, that statutory provision defines as a criminal violation the knowing unauthorized access or use of the system for any un

[114] 18 U.S.C. § 1030(a)(3).

[115] *See supra* Without Authorization and Exceeds Authorized Access

[116] *Id.*

[117] As noted in S. REP. NO. 99-432, at 7 (1986):

> The Committee wishes to be very precise about who may be prosecuted under the new subsection

Computer: F1r8auUd. S.C. § 1030(a)(4)

118

119

120

121

122

123

gain for one

124

125 means that the offender is conscious of the natural consequences of his action (i.e., that it is likely that

---

(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 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

[118] 18 U.S.C. § 1030(a)(4) imposes criminal liability on whoever:

> [K]nowingly 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.

[119] *Id.*

[120] United States v. Bae, 250 F.3d 774, 775 (D.C. Cir. 2001).

[121] United States v. Iyamu, 356 F. Supp. 3d 810, 814 (D. Minn. 2018).

[122] United States v. Barrington, 648 F.3d 1178, 1184 (11th Cir. 2011).

[123] U.S. DEP TOF JUSTICE, *supra* note 9, at 27
section 1030. Very little case law under section 1030 exists as to its meaning, leaving open the question of how broadly a court will interpret th

[124] Fidlar Techs. v. LPS Real Estate Data Sols., Inc., 82 F. Supp. 3d 844, 851 (C.D. Ill. 2015) (quoting United States v. Henningsen, 387 F.3d 585, 590 91 (7th Cir. 2004)), a f, 810 F.3d 1075 (7th Cir. 2016); *see also* United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (Silverman J., dissenting) (concluding that § 1030(a)(4) requires specific intent to defraud). More generally, other federal courts that have concluded that to
broadly to wrongdoing rather than to the specific elements of common law fraud *see, e.g.*, Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008)

> (1) a representation; (2) its falsity; (3) its materiality; (4) the speaker's knowledge of its falsity or ignorance of its truth; (5) an intent that it be acted on by the person and in the manner reasonably contemplated; (6) the hearer's ignorance of its

Wilcox v. First Interstate Bank of Or., NA, 815 F.2d 522, 531 n.7 (9th Cir. 1987) (citing Rice v. McAlister, 519 P.2d 1263, 1265 (Or. 1974)).

[125] S. REP. NO. 99-432, at 10 (1986).

someone will be defrauded) and intends that those consequences should occur (i.e., he intends that someone should be defrauded [126]

[127]

[128]

[129]

[130]

[131]

[132]

[133]

[134] Although the concept of computer use as a thing of value is underdeveloped in case law, a Senate Report accompanying the 1986 Amendment to the CFAA provides some indication that computer use may be a thing of value where it reduces computer availability that would otherwise generate revenue for the computer owner through usage fees paid by valid users.[135] Although some observers have suggested that this idea is outmoded given the modern prevalence of computers and the corresponding decrease in the value of computer use,[136] the DOJ has suggested that it may still be possible for computer use to meet the $5,000 threshold in the case of recurring or continuing use of an expensive computer.[137] In any event, the $5,000 threshold for fraud solely resulting in computer use is intended
trespassing will be prosecuted as fraud. [138] As the same 1986 Senate Report observed, if every trespass were thought
obliterate the distinction between § 1030(a)(4) and the CFAA provisions that prohibit trespass.[139] In practice, it is difficult to invoke § 1030(a)(4) against a computer trespasser in the absence of other conduct, because courts may be reluctant to infer adequate proof of an intent to defraud from mere unauthorized computer access or even observation of data [140]

---

[126] *See* Doyle, *supra* note 23, at 50.

[127] 18 U.S.C. § 1030(a)(4).

[128] S. REP. NO. 99-432, at 9 (1986).

[129] *Id.*

[130] 18 U.S.C. § 1030(a)(4).

[131] U.S. DEP TOF JUSTICE, *supra* note 9, at 32.

[132] United States v. Czubinski, 106 F.3d 1069, 1078
for obtaining information beca he value of information is
government had to show that the information was valuable to [the defendant] in light of a f

[133] *Id.* at 1078.

[134] 18 U.S.C. § 1030(a)(4).

[135] S. REP. NO. 99-432, at 10 (1986 agrees that the mere use of a computer or computer service has a value all its own. Mere trespasses onto someone else
channel that he might otherwise be making available for a fee to an auth

[136] KERR, *supra* note 7, at 99.

[137] U.S. DEP TOF JUSTICE, *supra* note 9, at 32.

[138] *See* Doyle, *supra* note 23, at 51.

[139] S. REP. NO. 99-432, at 10 (1986).

[140] *Czubinski*, 106. F3d at 1075 (concluding that government did not adequately p . . . and, *a*

Damaging a Computer, 1030(a)(5)

[141]

[142]

[143]

[144]

[145]

[146]

[147]

[148]

encompasses a range of hacking activities, such as t]he transfer of operation or confidential

[149] Transmission may occur through use of the internet or

---

fortiori,
no evidence that defendant intended to use that information for anything other than browsing).

[141] 18 U.S.C. § 1030(a)(5) imposes criminal liability on:

> (a) Whoever--
>
> (5)(A) 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;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

[142] U.S. DEP T OF JUSTICE, *supra* note 9, at 35.

[143] *Id.*

[144] Cybersec. & Infrastructure Sec. Agency, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks* (last revised Nov. 20, 2019), https://us-cert.cisa.gov/ncas/tips/ST04-015.

[145] Press Release, U.S. Dep Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens (quoting statement of Assistant Attorney General Brian A. Benczkowski).

[146] Former Operator of Illegal Booter Services Sentenced for Conspiracy to Commit Computer Damage and Abuse (Nov. 15, 2019), https://www.justice.gov/opa/pr/former-operator-illegal-booter-services-sentenced-conspiracy-commit-computer-damage-and-abuse.

[147] , Former IT Employee of Transcontinental Railroad Sentenced to Prison for Damaging Ex- https://www.justice.gov/opa/pr/former-it-employee-transcontinental-railroad-sentenced-prison-damaging-ex-employer-s-computer.

[148] 18 U.S.C. § 1030(a)(5)(A).

[149] Beale, *supra* note 1, at 170 (quoting Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, 14 U. PITT. J. TECH. L. POL Y 158, 167 69 (2014)).

physical mediums like compact discs.[150]

151

152

153

154

155

conscious purpose of causing damage . . . to [the relevant] computer. [156]

157

158

clearly destructive behavior such as using a virus or worm or deleting data . . . [b]ut it may also include less obviously invasive conduct, such as flooding an [159] For example, one federal court concluded that damage occurred as a result of

[150] Beale, *supra* note 1, at 170 (citing Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. FED. 101 (2001)); *accord* United States v. Sullivan, 44 (4th Cir. 2002) (per curiam) (concluding that a transmission under 18 U.S.C. § 1030(a)(5)(A) occurred through insertion of code into a computer system that eventually found its way into hand-held computers); N. Tex. Preventive Imaging LLC v. Eisenberg, No. SA CV 96-71AHS(EEX), 1996 WL 1359212, at *6 (C.D. Cal. Aug. a disabling code by floppy computer disk may fall within . . . [§ 1030(a)(5)(A)], if

[151] *See, e.g.*, Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1035 (N.D. Ill. 2008) Plaintiffs acknowledge that the precise method of installation of the erasure program is unknown, the Seventh Circuit recognizes that the precise mode of transmission is

[152] U.S. DEP T OF JUSTICE, *supra* note 9, at 37.

[153] 18 U.S.C. § 1030(a)(5)(A).

[154] *See* QVC, Inc. v. Resultly, LLC, 99 F. Supp. 3d 525, 536 (E.D. Pa. 2015) (concluding that § 1030(a)(5)(A) requires defendant

[155] 18 U.S.C. § 1030(a)(5)(A).

[156] *accord* United States v. Carlson, 2006) (discussing § 1030(a)(5) prosecution and noting that although CFAA

[157] 18 U.S.C. § 1030(e)(8).

[158] *See* Berris, *supra* note **Error! Bookmark not defined.** occurs, for example, where a hacker causes a computer to behave in a manner contrary to the intentions of *accord* United States v. Yücel, 97 F. Supp. 3d 413, 420 (S.D.N.Y. 2015) (construing damage under § 1030(a)(5) to include instances where a For a more detailed examination of different examples of damage, see, e.g., KERR, *supra* note 7, at 107 08.

[159] United States v. Hutchins, 361 F. Supp. 3d 779, 794 (E.D. Wis. 2019) (alterations in original) (quoting Fidlar Tech. v. LPS Real Estate Data Sols., Inc., 810 F.3d 1075, 1084 85 (7th Cir. 2016)).

thousands of phone calls and e- o use their systems.[160]

[161]

[162]

[163]

[164] 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 [165] Federal courts disagree on whether proving interruption of service such as computer systems or files being rendered unavailable is a prerequisite to demonstrating loss.[166] In other words, some courts construe loss to include reasonable costs caused by offenses regardless of whether those offenses involve service interruption, but other courts more narrowly interpret loss under the CFAA as requiring service interruption.[167]

[160] *Pulte Homes, Inc.*, 648 F.3d at 299, 301.

[161] 18 U.S.C. § 1030(a)(5).

[162] *Id.*

[163] United States v. McCord, Inc., 143 F.3d 1095, 1098 (8th Cir. 1998) (quoting Farmer v. Brennan, 511 U.S. 825, 837 (1994)).

[164] For example, one federal court found that a plaintiff sufficiently alleged a civil § 1030(a)(5) violation with allegations that the defendant recklessly caused damage by unauthorized computer access where he deleted data from unts, and server. MSC Safety Sols., LLC v. Trivent Safety Consulting, LLC, No. 19-CV-00938-MEH, 2019 WL 5189004, at *4 (D. Colo. Oct. 15, 2019).

[165] KERR, *supra* note 7, at 120 25.

[166] *See, e.g.*, Brown Jordan Int l, Inc. v. Carmicle, 846 F.3d 1167, 1173 74 (11th Cir. 2017) (comparing jurisdictions that construe loss broadly to include any costs of responding to an offense regardless of whether there was an interruption of service with those that narrowly construe loss as resulting only from an interruption of service).

[167] *Compare id.* (adopting broad view of loss that includes reasonable costs of responding to an offense even where there was no interruption of service) *and* Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC, 774 F.3d 1065, 1073 (6th Cir. 2014) (holding that loss under the CFAA includes both consequential damages caused by service interruption and reasonable costs of responding to an offense such as damage assessments) *with* Gen. Sci. Corp. v. SheerVision, Inc., No. 10-CV- covers lost revenue if the loss occurred as a result of interrupted service. *and* CoStar Realty Info., Inc. v. Field, 737 F. Supp. interruption of service in order for lost revenue to con

Password Trafficking (§ 1030(a)(6))

[168] [169] aimed at penalizing conduct associated with pirate unauthorized access to others [170] assuming an appropriate jurisdictional nexus discussed below, traffic knowingly and with intent to defraud in any password or similar information through which a computer may be accessed without authorization. [171] For the purposes of [172] A defendant need not intend to profit to engage in trafficking for § 1030(a)(6) purposes, but he must intend to transfer or dispose of the passwords or similar information.[173] meaning as in § 1030(a)(4), discussed above, and generally refers to acts undertaken with the knowledge that defrauding another is a likely consequence, and the intent that such fraud should actually occur.[174] [s] or [175] is a broad category intended to include explanations on how to access others [176] satisfy one of two jurisdictional hooks. First, § 1030(a)(6) could apply where trafficking affects interstate or foreign commerce [177] Although undefined by the CFAA and underdeveloped in case law, at least some courts examining civil § 1030(a)(6) claims appear to have construed the interstate or foreign commerce requirement broadly.[178] For example, for at least one court, trafficking involving the internet could satisfy the requirement.[179] Second, § 1030(a)(6) may also apply where the defendant traffics computer . . . used by or for the Government of the United States [180] Again there is no statutory definition

[168] 18 U.S.C. § 1030(a)(6) imposes criminal liability on:

> (a) 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.

[169] *See* Doyle, *supra* note 23, at 69.

[170] S. REP. NO. 99-432, at 13 (1986).

[171] 18 U.S.C. § 1030(a)(6).

[172] *Id.* § 1029(e)(5); *see id.* § 1030.

[173] U.S. DEP TOF JUSTICE, *supra* note 9, at 50.

[174] *See supra* Computer Fraud: 18 U.S.C. § 1030(a)(4)

[175] 18 U.S.C. § 1030(a)(6).

[176] S. REP. NO. 99-432, at 13 (1986); *accord* U.S. DEP TOF JUSTICE, *supra* note 9 Therefore, prosecutors should

[177] 18 U.S.C. § 1030(a)(6)(A).

[178] *See* Tracfone Wireless, Inc. v. Simply Wireless, Inc., 229 F. Supp. 3d 1284, 1297 (S.D. Fla. 2017) (concluding that plaintiff stated claim under § 1030(a)(6) where trafficking implicated the internet and a telecommunications network).

[179] *Id.* Courts have reached similar conclusions when interpreting 18 U.S.C. § 1029, a credit card fraud statute that *See, e.g.*, United States v. Rushdan, 870 F.2d 1509, 1513 14 (9th Cir. 1989) (concluding that federal

[180] 18 U.S.C. § 1030(a)(6)(B).

and little interpretive case law, but according to the DOJ

181

182

183

184

Threats and Extortion § 1030(a)(7)

185

186

187

188

189

190

---

[181] U.S. DEP TOF JUSTICE, *supra* note 9, at 51.

[182] *See* Doyle, *supra* note 23, at 69

[183] 18 U.S.C. § 10

[184] Doyle, *supra* note 23 (quoting (18 U.S.C. § 1030)).

[185] 18 U.S.C. § 1030(a)(7) imposes criminal liability on:

> (a) 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--
>
> (A) threat to cause damage to a protected computer;
>
> (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
>
> (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

[186] *Id.*

[187] *See* S. REP. NO. 104-357, at 12 (1996).

[188] *Id.* (quoting statement of Attorney General to Sen. Leahy).

[189] *Id.*

[190] *See, e.g.*, Indictment, United States v. Savandi, No. 3:18-cr-00704-BRM, 2018 WL 6798078 (D.N.J. Nov. 27, 2018); Press Release, U.S. D e to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018),

[191]

[192]

threat[s] to cause damage to a protected computer. [193] Threats to cause damage might include threats interfer[e] in any way with the normal operation of the computer or system in question, such as [by] 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. [194]
information from a protected computer without authorization or in excess of authorization *or* to impair the confidentiality of information obtained from a protected computer without authorization or by excee [195] In other words, this second category includes extortionate threats to obtain information through unauthorized access to a protected computer, *or* to disclose information *already obtained* through unauthorized access into a protected computer.[196] For example, an individual may fall within this second category when he hacks into a protected computer, obtains sensitive information, and then threatens to disclose it unless his demands are met.[197] Third, it
other thing of value in relation to damage to a protected computer, where such damage was [198] An example of this type of threat is the use of ransomware to .[199]

https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public. The installation of such ransomware may also violate § 1030(a)(5). *See* Indictment, *Savandi*, No. 3:18-cr-00704-BRM, 2018 WL 6798078, *supra* note 190 (charging defendants under both 18 U.S.C. § 1030(a)(7)(C) and § 1030(a)(5)(A)).

[191] Press Release, U.S.
Kingdom to Face Charges in St. Louis (Dec. 18, 2019), https://www.justice.gov/opa/pr/member-dark-overlord-hacking-group-extradited-united-kingdom-face-charges-st-louis. *See also* Indictment, United States v. Wyatt, No. 4:17-cr-00522-RLW-SPM, 2017 WL 11530077 (E.D. Mo. Nov. 8, 2017).

[192] U.S. Government Employee Charged in Computer Hacking and Cyber Stalking Scheme (Aug. 19, 2015), https://www.justice.gov/opa/pr/former-us-government-employee-charged-computer-hacking-and-cyber-stalking-scheme; *see also* Indictment, United States v. Ford, No. 1 15-CR-319, 2015 WL 4980336 (N.D. Ga. Aug. 18, 2015).

[193] 18 U.S.C. § 1030(a)(7)(A).

[194] *See* S. REP. NO. 104-357, at 12 (1996).

[195] 18 U.S.C. § 1030(a)(7)(B) (emphasis added).

[196] *Id.*

[197] Indictment, *Ford*, No. 1 15-CR-319, 2015 WL 4980336, *supra* note 192.

[198] 18 U.S.C. § 1030(a)(7)(C).

[199] U.S. DEP TOF JUSTICE, *supra* note 9, at 54; *accord* S. REP. NO. 104-357, at 12 (1996) (discussing § 1030(a)(7) and [o]ne can imagine situations in which hackers penetrate a system, encrypt a database and then demand

200

201

202

203

204

205

206

Remedies and Penalties

207

208

209

210

[200] *See* Doyle, *supra* note 23, at 63 & n. 353 (quoting *H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007: Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary*, 110th Cong., 1st Sess. (2007) (statement of Acting Principal Deputy Assistant Attorney General Andrew Lourie)).

[201] 18 U.S.C. § 1030(a)(7).

[202] *Extortion*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[203] *See, e.g.*, Inplant Enviro-Sys. 2000 Atlanta, Inc. v. Lee, No. 1:15-CV-0394-LMM, 2015 WL 13297963, at *4 (N.D. Ga. June 9, 2015) (holding that plaintiff alleged a valid claim for § 1030(a)(7) violation where defendant allegedly demanded $137,705 for the return of mas).

[204] U.S. DEP'T OF JUSTICE, *supra* note 9, at 53.

[205] 18 U.S.C. § 1030(a)(7).

[206] *See Inplant Enviro-Sys. 2000 Atlanta, Inc.*, No. 1:15-CV-0394-LMM, 2015 WL 13297963, at *4 (concluding that plaintiff adequately stated a § 1030(a)(7) violation against defendant who transmitted extortiona interstate or foreign commerce, as [it was] *accord* United States v. Kammersell, 196 F.3d 1137, 1139 (10th Cir. 1999) (concluding in that interstate commerce element of 18 U.S.C. § 875(c) a federal threat statute was satisfied where defendant transmitted threat via instant message between computers in the same state, where it was routed to a server in a second state).

[207] those involving espionage or national security information, but the statute also expressly permits investigation by the United States Secret Service and any other agency with authority. 18 U.S.C. § 1030(d); *accord* FBI, *Cyber Crime*, https://www.fbi.gov/investigate/cyber (last visited July 27, 2020). The Department of Justice prosecutes CFAA violations. *See generally* U.S. DEP'T OF JUSTICE, *supra* note 9 (summarizing DOJ policies and guidance on CFAA prosecutions).

[208] 18 U.S.C. § 1030.

[209] *Id.* § 1030(c)(2)(A).

[210] *Id.* § 1030(c)(3)(A).

211

212

s eTæa b2l Tea b3l e

T a b4l e

s eTæa b2l 2e3

s eTæa b3l Tea b4l e

214

Table 1. Overview of CFAA Maximum Penalties

Maximum Prison Terms by Subsection for First and Subsequent Offenses

Section*	Description	First Offense**	Subsequent Offense***
1030(a)(1)	Cyber Espionage	10 Years	20 Years
1030(a)(2)	Obtaining Information by Unauthorized Computer Access	1 Year (M); 5 Years (F)	10 Years
1030(a)(3)	Government Computer Trespassing	1 Year	10 Years
1030(a)(4)	Computer Fraud	5 Years	10 Years
1030(a)(5)(A)	Knowing Transmission + Intentional Damage to Computer	1 Year (M); 10 Years (F)	20 Years
1030(a)(5)(B)	Intentional Access + Reckless Damage to Computer	1 Year (M); 5 Years (F)	20 Years
1030(a)(5)(C)	Intentional Access + Damage to Computer + Loss	1 Year	10 Years
1030(a)(6)	Password Trafficking	1 Year	10 Years
1030(a)(7)	Threats and Extortion	5 Years	10 Years

Source: 18 U.S.C. § 1030(c).

Notes:

* Bolded subsection authorizes additional penalties beyond those reflected in this Table where there are certain aggravating factors such as causing death, broken down in further detail in **Table 3**.

** (M) denotes misdemeanor; (F) denotes felony. CFAA subsections that may be charged as a misdemeanor or a felony are broken down in further detail in **Table 2**, **Table 3**, and **Table 4**.

*** Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

211 *Id.* § 1030(c)(1)(A).

212 *Id.* § 1030(c)(1)(B).

213 *Id.* § 1030(c)(2)(B).

214 *Id.* §§ 1030(c)(4)(E) (F).

Table 2. Overview of Maximum Penalties Under 18 U.S.C. § 1030(a)(2)

Maximum Prison Terms for Obtaining Information by Unauthorized Computer Access

Description of Offense Under § 1030(a)(2)	Classification	Sentence
First Offense (No Special Conditions)	Misdemeanor	1 Year
Offense with One of Three Special Conditions: 1. Offense committed for purpose of commercial advantage or private financial gain; 2. Offense committed in furtherance of any criminal or tortious act in violation of the Constitution or state or federal law; or 3. The Value of the information obtained is greater than $5,000.	Felony	5 Years
Subsequent Offense*	Felony	10 Years

Source: 18 U.S.C. § 1030(c)(2)(C).

Note: * Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

Table 3. Overview of Maximum Penalties Under 18 U.S.C. § 1030(a)(5)(A)

Maximum Prison Terms for Knowing Transmission + Intentional Damage to a Computer

Description of Offense Under § 1030(a)(5)(A)	Classification	Sentence
First Offense (No Special Harms)	Misdemeanor	1 Year
First Offense with One of Six Special Harms: 1. Minimum loss of $5,000 to at least one person during a one year period; 2. Modification/impairment/potential modification or impairment of medical examination, diagnosis, treatment, or care of at least one individual; 3. Physical injury to any person; 4. Threat to public health or safety; 5. Damage affecting a computer used by or for the federal government in furtherance of the administration of justice, national defense, or national security; or 6. Damage affecting at least 10 protected computers in a 1-year period.	Felony	10 Years
Subsequent Offense*	Felony	20 Years
Offense where defendant knowingly/recklessly causes serious bodily injury, or attempts to do so	Felony	20 Years
Offense where defendant knowingly/recklessly causes death, or attempts to do so	Felony	Life Imprisonment

Source: 18 U.S.C. § 1030(c)(4).

Note: * Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

Table 4. Overview of Maximum Penalties Under 18 U.S.C. § 1030(a)(5)(B)

Maximum Prison Terms for Intentional Access + Reckless Damage to a Computer

Description of Offense Under § 1030(a)(5)(B)	Classification	Sentence
First Offense (No Special Harms)	Misdemeanor	1 Year
First Offense with One of Six Special Harms: 1. Minimum loss of $5,000 to at least one person during a one year period; 2. Modification/impairment/potential modification or impairment of medical examination, diagnosis, treatment, or care of at least one individual; 3. Physical injury to any person; 4. Threat to public health or safety; 5. Damage affecting a computer used by or for the federal government in furtherance of the administration of justice, national defense, or national security; or 6. Damage affecting at least 10 protected computers in a 1-year period.	Felony	5 Years
Subsequent Offense*	Felony	20 Years

Source: 18 U.S.C. § 1030(c)(4).

Note: * Subsequent offense refers to maximum penalties possible for offense committed following conviction for another CFAA offense.

Under a civil CFAA claim, the plaintiff can obtain compensatory damages and injunctive relief or other equitable relief.[215] However, civil actions are only possible if the violation results in certain types of losses or damages, such as physical injury, a threat to public health or safety, damage to 10 or more protected computers within the span of a year, or certain losses with a total value of at least $5,000.[216]

[217]

Selected CFAA Issues in the 116th Congress

[218]

[215] *Id.* § 1030(g).

[216] *Id.*

is beyond the scope of this Report. For a more detailed examination, see Doyle, *supra* note 23.

[217] *Id.* § 1030(j). A more detailed examination of the laws governing forfeiture is beyond the scope of this Report. For an analysis of forfeiture, including under § 1030, see CRS Report 97-139, *Crime and Forfeiture*, by Charles Doyle.

[218] *See infra* Hacking Back

219

220

221

222

223

The CFAA and ToS Violations

224

225

226

227 228 229 230

219 *Id.*

220 Beale, *supra* note 1, at 173 (quoting Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 239 (2014)); *accord* United States v. Gasperini, 894 F

221 *See infra* Botnet Trafficking

222 *See infra* The CFAA and ToS Violations

223 *Id.*

224 Berris, *supra* note 14. More broadly, legal commentators have described this issue as whether the CFAA imposes - KERR, *supra* note 7, at 51.

225 Berris, *supra* note 14.

226 *Id.*

227

228 United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system . . . at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a

229 LLC v. Citrin, 440 F.3d 418, 420 21 (7th Cir. 2006) (concluding that defendant lacked authorization after breaching duty of loyalty to employer).

230 United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (concluding that defendant exceeded authorized access by violating employer policy against using employer database for personal purposes).

United States v. Rodriguez[231]

[232]

[233]

[234]

[235] [236] [237]

[238]

[239]

customer data

[240]

purposes

purposes access

purposes [241]

[242]

[231] This report references a significant number of decisions by federal appellate courts of various regional circuits. For purposes of brevity, references to a particular circuit in the body of this report (e.g., the First Circuit) refer to the U.S. Court of Appeals for that particular circuit.

[232] *Rodriguez*, 628 F.3d at 1263.

[233] *John*, 597 F.3d at 272.

[234] Berris, *supra* note 14.

[235] United States v. Valle, 807 F.3d 508, 523 (2d Cir. 2015) (concluding that an individual does not exceed authorized access where individual is authorized for certain uses, and surpasses those).

[236] t they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is

[237]

[238] *See Valle*, 807 F.3d at 528.

[239] *Nosal*, 676 F.3d at 856 57.

[240] *Id.* at 857.

[241] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) Second, a violation of the terms of use of a website without more

[242] *Id.*

243

244

Van Buren

v. United States[245] [246] Van Buren,

247

Van Buren [248]

Van Buren

249

250

251

252

Botnet Trafficking

253

254

---

243 *Nosal*, 676 F.3d at 859, 861.

244 Berris, *supra* note 14.

245 Van Buren v. United States, 206 L. Ed. 2d 822 (Apr. 20, 2020).

246 United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, No. 19-783, 2020 WL 1906566 (Apr. 20, 2020).

247 *Id.* at 1197 98, 1208.

248 *October Term 2020*, SCOTUSBLOG, https://www.scotusblog.com/case-files/terms/ot2020/?sort=mname (last visited Sept. 9, 2020).

249 H.R. 2454, 113th Cong. (2013).

250 *Id.*

251 Press Release, U.S.
2013), https://lofgren.house.gov/media/press-releases/rep-zoe-lofgren-introduces-bipartisan-aarons-law.

252 H.R. 2454, 113th Cong. (2013).

253 Beale, *supra* note 1, at 173 (quoting Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 239 (2014)); *accord* United States v. Gasperini, 894

254 *See* Beale, *supra* note 1 internet may be used to disrupt the internet

255 256

257

n o t

258

259

260

261

262

263

264

265

266

267

255 U.S. *Prosecuting the Sale of Botnets and Malicious Software* (Mar. 18, 2015), https://www.justice.gov/archives/opa/blog/prosecuting-sale-botnets-and-malicious-software.

256 *See* Matwyshyn, *supra* note 13

257 *Prosecuting the Sale of Botnets*, *supra* note 255.

258 *Id.*; *accord* Triana, *supra* note 13, at 1315 (discussing uncertainty of whether sale of botnets and malware would violate the CFAA).

259 *Prosecuting the Sale of Botnets*, *supra* note 255.

260 *See id.* While trafficking in botnets is sometimes chargeable under other subsections of the Computer Fraud and Abuse Act, [the problem of individuals trafficking in botnets that they did not create] has resulted in, and will increasingly result in, the inability to prosecute individuals selling access to thousands of infected

261 18 U.S.C. § 1030(a)(6).

262 *Id.* § 1030(a)(5).

263 *See* Triana, *supra* note 13 Since hackers selling malware more clearly intend to profit off of their skills, they likely do not meet the mens rea r

264 *See, e.g.*, Press Release, U.S. Marcus Hutchins Pleads Guilty to Creating and Distributing the Kronos Banking Trojan and UPAS Kit Malware (May 3, 2019), https://www.justice.gov/usao-edwi/pr/marcus-hutchins-pleads-guilty-creating-and-distributing-kronos-banking-trojan-and-upas.

265 *Id.*; Press Release, U.S.
Global Botnet Conspiracy (Aug. 3, 2017), https://www.justice.gov/opa/pr/russian-citizen-sentenced-46-months-prison-involvement-global-botnet-conspiracy.

266 *See* Press Release, U.S.
Botnets (Sept. 6, 2012), https://www.justice.gov/opa/pr/arizona-man-sentenced-30-months-prison-selling-access-botnets.

267 *See* Press Release, *supra* note 264.

268

269

270

271 272

273

274 275

276

277

278

279

280

281

282

[268] United States v. Smith, 950 F.3d 893, 895 (D.C. Cir. 2020) (citing United States v. Gatling, 96 F.3d 1511, 1518 (D.C. Cir. 1996)). For a detailed examination of federal conspiracy law, *see, e.g.*, CRS Report R41223, *Federal Conspiracy Law: A Brief Overview*, by Charles Doyle.

[269] *See supra* note 263 and accompanying discussion.

[270] *Id.*

[271] 18 U.S.C. § 371.

[272] *See supra* Remedies and Penalties

[273] Tex. Bus. & Com. Code Ann. § 324.055 (West).

[274] President Barack Obama, Remarks by the President at the National Cybersecurity Communications Integration Center (Jan. 13, 2015), *reprinted at* proposing to update the authorities that law enforcement uses to go after cyber criminals. We want to be able to better prosecute those who are involved in cyber attacks, those who are involved in the sale of cyber weapons like botnets

[275] *See, e.g.*, Defending American Security from Kremlin Aggression Act of 2019, S. 482, 116th Cong. (2019).

[276] *Id.*

[277] The relevant provision is titled *Id.* § 406.

[278] *Id.*

[279] *Id.*

[280] *Id.*

[281] S. 2931, 114th Cong. (2016).

[282] Letter from Access Now et al., to Senate (June 1, 2016), https://www.eff.org/document/coalition-letter-opposing-botnet-prevention-act.

283

Hacking Back

284 285 286 287

288 289

290

291

292

293

283 *See* *Prosecuting the Sale of Botnets*, *supra* note 255 (defending proposal to prohibit botnet trafficking on grounds that to prove, beyond a reasonable doubt, that the individual intentionally undertook an act (trafficking in a means of access) that he or she knew to be

284 *See, e.g.*, U.S. DEP T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 23 (2018), https://www.justice.gov/criminal-ccips/file/1096971/download#page=23 (discussing hacking back).

285 *See, e.g.*, Shane Huang, *Proposing A Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1233 (2014).

286 *See, e.g.*, Nicholas Schmidle, *Vigilantes Who Hack Back*, NEW YORKER (Apr. 30, 2018), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

287 *See, e.g.*, Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019).

288 *See* Beale, *supra* note 1

Id. at 190 (quoting Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?* 20 RICH. J.L. & TECH. 12, 4 (2014)).

289 *Compare* Josephine Wolff, *Attack of the Hack Back*, SLATE (Oct. 17, 2017), https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html (proclaiming *and* Martin Giles, Five Reasons "Hacking Back" is *Cybersecurity Chaos*, MIT TECH. REV. (June 21, 2019), https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/ (describing *with* KERR, *supra* note 7, at 133 (summarizing debate over hacking back and collecting articles arguing in favor of hacking back) *and* *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV

West could not reliably count on the local sheriff to protect them, and instead kept a weapon handy to stymie potential aggressors, Internet users may need to

290 Josephine Wolff, *When Companies Get Hacked, Should They Be Allowed to Hack Back?*, ATLANTIC (July 14, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/ (summarizing concern of e as a vehicle for more attacks and greater chaos, particularly if victims incorrectly identify who is attacking them, or even invent or stage fake attacks from adversaries as an excuse

291 *See, e.g.*, Beale, *supra* note 1, at 198 (summarizing view that due to difficulty in accurately attributing the source of a cyber-

292 *See* PATRICK LIN, ETHICS OF HACKING BACK: SIX ARGUMENTS FROM ARMED CONFLICT TO ZOMBIES 15 (2016), http://ethics.calpoly.edu/hackingback.pdf

misinterpreted by the receiving nation as a military response from our state, to serious political and economic

293 *See, e.g.*, CTR. FOR CYBER & HOMELAND SEC., GEO. WASH. UNIV., INTO THE GRAY ZONE: THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS 27 (2016), http://cchs.auburn.edu/_files/into-the-gray-zone.pdf

unauthorized and rightly *accord* Giles, *supra* note 289 (critiquing hacking back).

294

295

296

297

298

299

300

294 Press Release, Congressman Tom Graves, Graves, Gottheimer Introduce the Active Cyber Defense Certainty Act (June 13, 2019), https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=401122.

295 Beale, *supra* note 1, at 191.

296 *See, e.g.*, U.S. DEP T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE, *supra* note 284, at 23 (cautioning that t own s and foreign countries, if the accessed computer is located

The CFAA has a carve out for certain law enforcement activity, which provides that:
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 C. § 1030(f).

Although beyond the scope of this Report, it is worth observing that the federal wiretapping statute, 18 U.S.C. § 2511, contains the following carve out applicable to certain acts of hacking back conducted under color of law:

> (i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--
>
> (I) the owner or operator of the pr communications on the protected computer;
>
> (II) the person acting under color of law is lawfully engaged in an investigation;
>
> (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer
>
> (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C. § 2511(2)(i).

297 *E.g.*, U.S. DEP T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE, *supra* note 284, at 23; Orin Kerr, *The Legal Case Against Hack-Back: A Response to Stewart Baker*, STEPTOE CYBERBLOG (Nov. 2, 2012), https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/; Beale, *supra* note 1, at 191; CTR. FOR CYBER & HOMELAND SEC., GEO. WASH. UNIV., *supra* note 293; *but see* Stewart Baker, *RATs and Poison Part II: The Legal Case for Counterhacking*, STEPTOE CYBERBLOG (Nov. 2, 2012), https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ (arguing that hacking back may not be a violation of the CFAA).

298 Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019).

299 *Id.*

300 *Id.*

301
302

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in

[301] *Id.*

[302] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).