Congressional Research Service
Informing the legislative debate since 1914

Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes

May 16, 2023

Congressional Research Service
https://crsreports.congress.gov
R47557

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47557

May 16, 2023

Peter G. Berris
Legislative Attorney

Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes

There is no single, straightforward definition of cybercrime under federal law. Rather, depending on the context, "cybercrime" may refer to all crimes involving computers, or only to crimes targeting computers, or to crimes unique to the computer context. Regardless, federal prosecutors have a number of statutory tools to charge conduct that fits within these varying conceptualizations of cybercrime.

One example of a federal cybercrime provision is the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030—a law prohibiting a variety of computer-related conduct and providing for both civil and criminal penalties. Although sometimes described as an anti-hacking law, the CFAA covers more than just hacking. The statute prohibits seven categories of conduct involving unauthorized access to computers, including, with certain exceptions and conditions:

- Obtaining national security information through unauthorized computer access and sharing or retaining it;
- Obtaining certain types of information through unauthorized computer access;
- Accessing government computers without authorization;
- Engaging in computer-based frauds through unauthorized computer access;
- Knowingly causing damage to certain computers by transmission of a program, information, code, or command;
- Trafficking in passwords or other means of unauthorized access to a computer;
- Making extortionate threats to harm a computer or based on information obtained through unauthorized access to a computer.

In addition to hacking, some types of cybercrime may include data theft, swatting, doxing, cyberstalking, cyber harassment, unlawful access to electronic communications, or fraud. To the extent that conduct in these categories involves unauthorized computer access, the CFAA may provide a powerful statutory tool to prosecute. Depending on the circumstances, prosecutors may also look to a number of other statutes in their charging decisions. For example, data theft targeting trade secrets may violate the Economic Espionage Act. Cyber harassment and cyberstalking might run afoul of the federal cyberstalking statute (18 U.S.C. § 2261A(2)). Swatting—that is, reporting a false emergency in an attempt to direct an armed police response to a target or location—may violate a federal law proscribing the transmission of certain threats in interstate commerce. When it targets certain federal officials, doxing—obtaining another individual's personal identifying information (such as an address, telephone number, or Social Security Number) and posting it online for harassment or other purposes—may incur penalties under a federal statute restricting the disclosure of personal information. The unlawful access of communications—such as emails and texts—might potentially violate statutes such as the Wiretap Act. Finally, one frequently used prosecutorial tool relevant to the cybercrime context is the federal wire fraud statute, 18 U.S.C. § 1343, which authorizes criminal penalties for knowing or willing participation in a scheme to defraud using interstate wires. The wire fraud statute provides an additional statutory tool to prosecute some conduct that may also violate the CFAA, and an alternate tool to charge electronic fraud that does not involve unauthorized computer access as required by the CFAA's cyber-fraud provisions.

The ubiquity of computers—and the myriad ways in which they may be used or targeted by criminals—means there is no shortage of cybercrime issues of potential legislative interest to Congress. For example, Congress may wish to consider creating new criminal penalties for conduct like doxing or trafficking in botnets (networks of compromised computers used to perpetrate various cybercrimes). Congress may also be interested in establishing additional penalties for cybercrimes with particular targets such as those impacting critical infrastructure. Alternatively, Congress may seek solutions outside of criminal law to provide for other means of responding to cybercrimes—as in the case of legislative proposals that would explore or facilitate hacking back against cyber attackers. In recent Congresses, Members have introduced proposals on each of these topics.

Contents

Tables

Contacts

Introduction

Computers are more prevalent than ever before.[1] Their ubiquity has made them a favored tool for, and target of, criminals.[2] In 2022—the most recent year for which data is available—the FBI's Internet Crime Complaint Center received 800,944 reported complaints of cybercrime with potential "losses exceeding $10.3 billion."[3] Numerous headline-grabbing incidents further underscore the frequent and evolving connection between computers and crime. For example, in May 2021, a ransomware attack prompted the Colonial Pipeline Company to shut down its network temporarily, impacting gasoline availability and prices[4] before the company reportedly paid a ransom of over $4 million worth of Bitcoin.[5] In January 2022, the International Committee of the Red Cross announced that cyber attackers had obtained "personal data belonging to more than 515,000 people worldwide" from its systems.[6] In March 2022, hackers reportedly stole cryptocurrency valued in the hundreds of millions of dollars from a service called Ronin.[7] In December 2022, federal authorities arrested two Queens, New York residents, whom they alleged conspired with Russian hackers to "hack the electronic taxi dispatch system" at John F. Kennedy

[1] According to the United States Census Bureau (Census Bureau), by one measure, only 8% of households had a computer in 1984. MICHAEL MARTIN, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2018, at 4 (2021), https://www.census.gov/content/dam/Census/library/publications/2021/acs/acs-49.pdf. According to the same report, 92% of households had a computer in 2018. *Id.* The prevalence of computers may also be inferred from the estimated number of computerized devices such as smart appliances and fitness trackers connected to the Internet of Things (IoT)—by one account, there will be 21.5 billion such active devices connected to the IoT by 2025. CRS In Focus IF11239, *The Internet of Things (IoT): An Overview*, by Patricia Moloney Figliola. 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 (2018). As discussed below, these devices are considered computers in the context of the CFAA. *See infra* Section "Protected Computers."

[2] *See, e.g.*, *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. 5–9 (2022) (statement of Christopher A. Wray, Director, Fed. Bureau of Investigation) (discussing nature of current cyber threats).

[3] FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2022, at 7 (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf; *see also*, Press Release, Fed. Bureau of Investigation Springfield, Internet Crime Complaint Center Releases 2022 Statistics (Mar. 22, 2023), https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.

[4] CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran; *see generally* Stephanie Kelly & Laura Sanicola, *U.S. Capital Running Out of Gas, Even as Colonial Pipeline Recovers*, REUTERS (May 14, 2021), https://www.reuters.com/business/energy/colonial-pipeline-ramps-up-us-seeks-emerge-fuel-crunch-2021-05-14/; Brett Molina & Nathan Bomey, *Colonial Pipeline Restarted Operations, Owners Say "It Will Take Several Days" For Supply Chain to Return to Normal*, USA TODAY (May 12, 2021), https://www.usatoday.com/story/money/2021/05/12/gas-shortage-gas-prices-colonial-pipeline-nc-virginia-north-carolina/5052551001/; Catherine Thorbecke, *Gas Hits Highest Price in 6 Years, Fuel Outages Persist Despite Colonial Pipeline Restart*, ABC NEWS (May 17, 2021), https://abcnews.go.com/US/gas-hits-highest-price-years-fuel-outages-persist/story?id=77735010.

[5] Cathy Bussewitz, *Colonial Pipeline Confirms It Paid $4.4M to Hackers*, AP NEWS (May 19, 2021), https://apnews.com/article/hacking-technology-business-ed1556556c7af6220e6990978ab4f745.

[6] *Cyber-attack on ICRC: What we Know*, INT'L COMM. OF THE RED CROSS (Feb. 16, 2022), https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

[7] Rob Lever, *Data Breaches in 2022*, U.S. NEWS & WORLD REPORT (Oct. 28, 2022), https://www.usnews.com/360-reviews/privacy/recent-data-breaches; Tom Wilson & Elizabeth Howcroft, *Blockchain Project Ronin Hit by $615 Million Crypto Heist*, REUTERS (Mar. 29, 2022), https://www.reuters.com/technology/blockchain-company-ronin-hit-by-615-million-crypto-heist-2022-03-29/.

International Airport and used their unauthorized access to charge drivers a fee to skip the taxi queue.[8]

The world of computer-based crime extends beyond financially motivated hacking. Examples abound of criminals using computers and the internet to threaten[9] and stalk,[10] among other things.

Conceptually, the true scope of cybercrime or computer crime depends in part on definitions.[11] Depending on the context, "cybercrime" might refer specifically to crimes requiring the use of a computer, such as hacking, or to traditional crimes when they involve use of a computer or the internet, like harassment.[12] This report uses the term cybercrime somewhat broadly to include both crimes unique to the computer context and some traditional crimes that may be committed using computers.[13] The report focuses mainly on the Computer Fraud and Abuse Act (CFAA)—a primary tool in prosecuting cybercrimes like hacking and ransomware attacks at the federal level.[14] The report discusses key CFAA terms and summarizes its substantive prohibitions, then provides an overview of remedies and penalties under the statute. Many cybercrimes may implicate federal statutes other than, or in addition to, the CFAA.[15] Thus, the report briefly discusses some of these crimes, such as cyberstalking, and identifies statutes that may be used to

[8] Indictment, United States v. Abayev, No. 22 Crim. 655 (S.D.N.Y. Dec. 5, 2022); Press Release, U.S. Dep't of Just., Two Men Arrested For Conspiring With Russian Nationals To Hack The Taxi Dispatch System At JFK Airport (Dec. 20, 2022), https://www.justice.gov/usao-sdny/pr/two-men-arrested-conspiring-russian-nationals-hack-taxi-dispatch-system-jfk-airport.

[9] *E.g.*, Press Release, U.S. Dep't of Just., Connecticut Man Pleads Guilty to Cyberstalking and Threatening Massachusetts Woman (Sep. 7, 2022), https://www.justice.gov/usao-ma/pr/connecticut-man-pleads-guilty-cyberstalking-and-threatening-massachusetts-woman; Press Release, U.S. Dep't of Just., Man Arrested for Making Threats of Violence Against FBI (Aug. 15, 2022), https://www.justice.gov/opa/pr/man-arrested-making-threats-violence-against-fbi; Press Release, U.S. Dep't of Just., New Jersey Man Pleads Guilty to Threatening Employees of Latino Civil Rights Organizations (Oct. 20, 2010), https://www.justice.gov/opa/pr/new-jersey-man-pleads-guilty-threatening-employees-latino-civil-rights-organizations.

[10] *E.g.*, Press Release, U.S. Dep't of Just., Two Former eBay Employees Sentenced for Aggressive Cyberstalking Campaign (Oct. 11, 2022), https://www.justice.gov/usao-ma/pr/two-former-ebay-employees-sentenced-aggressive-cyberstalking-campaign; Press Release, U.S. Dep't of Just., Deputy U.S. Marshal Charged with Cyberstalking and Perjury (Mar. 14, 2021), https://www.justice.gov/opa/pr/deputy-us-marshal-charged-cyberstalking-and-perjury; Press Release, U.S. Dep't of Just., Florida Man Sentenced for Racially-Motivated Interference with Election in Charlottesville, Virginia and for Cyberstalking in Florida (Aug. 31, 2020), https://www.justice.gov/opa/pr/florida-man-sentenced-racially-motivated-interference-election-charlottesville-virginia-and.

[11] This report uses the phrases cybercrime and computer crime interchangeably.

[12] *See, e.g.*, ORIN S. KERR, COMPUTER CRIME LAW 1 (5th ed. 2022) ("Substantive computer crime law divides into two basic categories: computer misuse crimes and traditional crimes."); COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (defining computer crime, cybercrime, and network crime in relation to " those crimes that use or target computer networks"); *Crime*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining computer crime as "[a] crime involving the use of a computer, such as sabotaging or stealing electronically stored data"); *Cybercrime*, NEW OXFORD AMERICAN DICTIONARY (1st ed. 2005) (defining cybercrime as "crime conducted via the Internet or some other computer network"); *Cybercrime*, BRITANNICA (2022), https://www.britannica.com/topic/cybercrime (defining cybercrime, "also called computer crime," as "the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy").

[13] For further discussion of how to conceptualize cybercrime, see generally KERR, *supra* note 12, at 1–3.

[14] *See* U.S. DEP'T OF JUST., JUSTICE MANUAL § 9-48.000 (2022), https://www.justice.gov/jm/jm-9-48000-computer-fraud (describing importance of CFAA in "address[ing] cyber-based crimes").

[15] Given the large number of federal criminal provisions, it is not possible to provide a comprehensive overview of federal laws that may apply to every example of crime involving computers. *See, e.g.*, Van Buren v. United States, 141 S. Ct. 1648, 1669 (2021) (Thomas, J., dissenting) ("The number of federal laws and regulations that trigger criminal penalties may be as high as several hundred thousand.").

prosecute them at the federal level. The report concludes with a discussion of congressional considerations.

The Computer Fraud and Abuse Act

Congress was prescient about the ubiquity of cybercrime nearly 40 years ago when it enacted the CFAA—a civil[16] and criminal law that prohibits a range of computer-based acts.[17] While a number of federal statutes may be relevant to combatting nefarious computer activities such as those discussed above,[18] the CFAA is perhaps the most relevant.[19]Among other things, the CFAA prohibits a person from trespassing into, damaging, or acquiring information from certain categories of computers, assuming the user lacks authorization for that conduct.[20] Prosecutors invoke the CFAA to combat a variety of malign computer-based activities.[21]

History of the CFAA

By many accounts, the history of the CFAA begins with a movie—the 1983 thriller *WarGames*[22] starring Matthew Broderick.[23] In *WarGames*, Broderick's character, a rebellious high school student, nearly starts World War III when he accidentally accesses the computer system controlling the United States nuclear arsenal, mistaking the system for an interactive video game.[24] The movie's depiction of the dangers of the computer age—where even nuclear annihilation could be a few keystrokes away—was not lost on policy makers.[25] According to one

[16] This report cites to civil CFAA opinions despite focusing on cybercrime, as "most of the published cases interpreting § 1030 arise in the civil context rather than the criminal context." KERR, *supra* note 12, at 31. Further, courts "must interpret the statute consistently, whether [they] encounter its application in a criminal or noncriminal context." hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1200 (9th Cir. 2022) (quoting Leocal v. Ashcroft, 543 U.S. 1, 12 n.8, (2004); *see also* ORIN S. KERR, COMPUTER CRIME LAW 75 (3d ed. 2013) ("Courts generally use civil and criminal interpretations of federal statutes interchangeably absent an indication that Congress intended a contrary approach.").

[17] H.R. REP. NO. 98-894, at 10 (1984) ("[B]y combining the ubiquity of the telephone with the capability of the personal computer, a whole new dimension of criminal activity becomes possible.").

[18] 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. *See infra* "Other Cybercrimes."

[19] *See, e.g.*, John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 418–19 (2016) (describing the CFAA as a "cornerstone" statute and the "most important" of the "wide array of statutes that address the full life cycle of a national security cyber threat"); Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 89 (2001) (naming the CFAA as "the single most important federal statute governing computer crime").

[20] 18 U.S.C. § 1030.

[21] *See infra* Section "Prohibited Conduct Under the CFAA."

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

[23] *See* Fred Kaplan, *'WarGames' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. TIMES (Feb. 19, 2016), https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html (describing the birth of federal cybersecurity laws following President Ronald Reagan's concern over the movie); Ivan Evtimov, et al., *Is Tricking A Robot Hacking?*, 34 BERKELEY TECH. L.J. 891, 904 (2019) ("According to popular lore, President Reagan saw the movie *War Games* and met with his national security advisers the next day to discuss America's cyber vulnerabilities. The CFAA is said to be the result of their deliberations."); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 492 (2012) ("There is some evidence that when the CFAA was originally enacted in 1984, it was partially in response to the situations depicted in the action film WarGames.").

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

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

report, after viewing *WarGames* at Camp David, President Ronald Reagan asked advisers and the chairman of the Joint Chiefs of Staff whether the plot of the movie was possible.[26] The CFAA is sometimes "said to be the [eventual] result of their deliberations,"[27] although congressional interest in computer crimes may be traced back at least as far as the 1970s.[28]

The first major federal computer-crime enactment came in the form of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the 1984 Act).[29] With exceptions, the law prohibited three subsets of computer-based conduct: (1) obtaining national security information through unauthorized computer access; (2) obtaining financial information through unauthorized computer access; and (3) trespassing into a government computer and "knowingly us[ing], modif[ying], destroy[ing], or disclos[ing] information" on that computer.[30] The 1984 Act was relatively narrow,[31] and the Department of Justice (DOJ) expressed concern that it made computer crime prosecutions difficult.[32] In 1986, Congress substantially amended the 1984 Act, and the modern CFAA has many of its roots in that 1986 amendment.[33] Among other things, the 1986 amendment modified intent requirements and prohibited new categories of conduct including password trafficking, damaging computers, and accessing computers with intent to defraud.[34] Since 1986, Congress has amended the CFAA on numerous occasions,[35] broadening both the scope of conduct prohibited by the statute and the scope of computers protected.[36] Today, the CFAA is the main federal[37] computer misuse statute.[38]

---

[26] Kaplan, *supra* note 23.

[27] Evtimov, *supra* note 23, at 904.

[28] *E.g.*, S. COMM. ON GOV'T OPERATIONS, 94TH CONG., PROBLEMS ASSOCIATED WITH COMPUTER TECHNOLOGY IN FEDERAL PROGRAMS AND PRIVATE INDUSTRY—COMPUTER ABUSES (Comm. Print 1976).

[29] *See* WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012) ("In 1984, Congress initiated a campaign against computer crime by passing the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984."); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615 (2003) ("Congress enacted the first federal computer crime law in 1984.").

[30] P.L. 98-473, § 2102, 98 Stat. 1837 (1984) (codified at 18 U.S.C. § 1030).

[31] For instance, the 1984 Act "was limited to a narrow range of computers—namely, those containing national security information or financial data and those operated by or on behalf of the government." hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1197 (9th Cir. 2022).

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

[33] Kerr, *supra* note 29, at 1598 n.11, 1615.

[34] Computer Fraud and Abuse Act of 1986, P.L. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030).

[35] *E.g.*, Anti-Drug Abuse Act of 1988, P.L. 100-690, 102 Stat. 4181; Financial Institutions Reform, Recovery, and Enforcement Act of 1989, P.L. 101-73, 103 Stat. 183; Crime Control Act of 1990, Pub. L. No. 101–647, 104 Stat. 4789; Violent Crime Control Act of 1994, Pub. L. No. 103–322, 108 Stat. 1796 ; Economic Espionage Act of 1996, Pub. L. No. 104–294, 110 Stat. 3488; Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107–56,115 Stat. 272; 21st Century Department of Justice Appropriations Authorization Act, Pub. L. No. 107-273, 116 Stat. 1758 (2002); Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135; Former Vice President Protection Act of 2008, Pub. L. No. 110-326, 122 Stat. 3560.

[36] *See* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 1–2.

[37] 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 (1999). Computer misuse statutes have been enacted in "all fifty states.... " KERR, *supra* note 12, 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 (surveying computer crime laws of all 50 states).

[38] *See* KERR, *supra* note 12, at 30 (describing CFAA as "the federal computer misuse statute"); *see also* Evtimov, *supra* note 23, at 904 ("Since its implementation, the CFAA has been the nation's predominant anti-hacking law.").

Overview of the CFAA

Key CFAA Terms

Although prosecutors may use the CFAA to charge hacking,[39] and courts and observers have described the CFAA as an anti-hacking statute,[40] the word "hacking" does not appear in any of its various provisions.[41] Instead, the statute criminalizes several categories of conduct that include many types of computer hacking as well as a variety of other computer-based activities.[42] Generally, the CFAA prohibits certain conduct that is carried out by an individual "*without authorization*" or who "*exceeds authorized access*," and that involves a *computer* or a "*protected computer*."[43] Two criminal provisions impose liability for conduct relating to "*damage*" to a computer.[44] Thus, the scope of the CFAA turns largely on the meaning of these terms, which are discussed below.

Computer

The CFAA broadly[45] defines "computer" as any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions," including "any data storage facility or communications facility directly related to or operating in conjunction with such device.... "[46] The CFAA excludes only automated typewriters, typesetters, portable hand held calculators, and similar devices from its definition of computer.[47] These limited exceptions "show just how general" the statute's definition of computer is.[48] As one court explained, the definition includes any device with an electronic data processor, of which there are numerous examples.[49] Thus, under the CFAA, computers include not only laptops and desktops, but also a wide array of computerized devices ranging from cellphones to objects embedded with microchips, such as certain microwave ovens, watches, and televisions.[50]

Protected Computers

Several provisions of the CFAA specifically concern "protected computers."[51] Among other things, the CFAA defines protected computers as those that are either "exclusively for the use of a

[39] *See infra* Section "Prohibited Conduct Under the CFAA."

[40] *E.g.*, United States v. Nosal (*Nosal I*), 676 F.3d 854, 857 (9th Cir. 2012); Evtimov, *supra* note 23, at 904.

[41] *See* 18 U.S.C. § 1030 (proscribing various conduct without use of the word "hacking").

[42] *Id.*

[43] *See, e.g.*, *id.* § 1030(a)(2) (prohibiting "intentionally access[ing] a computer without authorization" or in excess of authorization, and obtaining certain types of information, including from a "protected computer" (emphasis added)).

[44] *Id.* § 1030(a)(5), (a)(7).

[45] *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).

[46] 18 U.S.C. § 1030(e)(1).

[47] *Id.*

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

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

[50] *Id.* at 902–03; *accord* United States v. Nosal (*Nosal II*), 844 F.3d 1024, 1050 (9th Cir. 2016) (Reinhardt, J., dissenting) ("This means that nearly all desktops, laptops, servers, smart-phones, as well as any 'iPad, Kindle, Nook, X–box, Blu–Ray player or any other Internet-enabled device,' including even some thermostats qualify as [protected computers]." (quoting United States v. Nosal *(Nosal I)*, 676 F.3d 854, 861 (9th Cir. 2012))).

[51] 18 U.S.C. § 1030.

financial institution or the United States Government" or that are "used in or affecting interstate or foreign commerce or communication.... "[52] Courts have construed the latter phrase to include any computer connected to the internet.[53] Thus, most modern computing devices are subject to the CFAA's protections, including devices such as smart appliances and fitness trackers connected to the Internet of Things[54]—"a system of interrelated devices connected to a network and/or to one another, exchanging data without necessarily requiring human-to-machine interaction."[55]

Another important type of computer that fits within the definition of protected computer is a server—a computer that manages website data and other information.[56] For example, one court concluded that the web servers storing and sharing the member data of a large social media website qualified as protected computers.[57]

Without Authorization and Exceeds Authorized Access

The CFAA applies only if the defendant acts "without authorization" or "exceeds authorized access."[58] For example, Section 1030(a)(2) prohibits intentionally accessing a computer without authorization or in excess of authorization and obtaining information from a financial institution, the federal government, or a protected computer.[59] Other provisions contain nearly identical requirements.[60]

---

[52] *Id.* § 1030(e)(2). A 2020 amendment to the CFAA expanded the definition of "protected computer" to include any computer that "is part of a voting system; and ... is used for the management, support, or administration of a Federal election; or ... has moved in or otherwise affects interstate or foreign commerce." Defending the Integrity of Voting Systems Act, Pub. L. 116-179, 134 Stat. 855 (2020) (codified in relevant part at 18 U.S.C. § 1030(e)(2)(C)).

[53] *See, e.g.*, Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (interpreting the definition of protected computer in the context of one subsection of the CFAA to include "all computers that connect to the Internet"); hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1195 (9th Cir. 2022) ("The term 'protected computer' refers to any computer 'used in or affecting interstate or foreign commerce or communication[]'—effectively any computer connected to the Internet." (quoting 18 U.S.C. § 1030(e)(2)(B)) (internal citations omitted)).

[54] Although federal cases specifically examining the CFAA's applicability in the context of the Internet of Things are scarce, a number of observers have concluded that internet-enabled objects qualify as protected computers. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577–78 (2010); *accord* Beale & Berris, *supra* note 1, at 170.

In one case, federal prosecutors used the CFAA to charge defendants who allegedly gained unauthorized access to Ring smart devices. Indictment, United States v. Nelson and McCarthy, No. 2:22-cr-00598-JAK (C.D. Cal. Dec. 16, 2022). Another example from case law is *United States v. Peterson*. 776 F. App'x 533 (9th Cir. 2019). In *Peterson*, the U.S. 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 under the CFAA, including "refrigerators with Internet connectivity, Fitbit™ watches" and certain automobiles. *Id.* at 535 n.3. Although the court did not discuss these devices in relation to the phrase "protected computer," it described them in a manner that would satisfy the definition of protected computer under the CFAA; as the court indicated, Internet of Things devices are (1) computers (2) connected to the internet. *Id.* at 534. For a similar example, see United States v. Wells, 29 F.4th 580, 588 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 267 (2022).

[55] CRS In Focus IF11239, *The Internet of Things (IoT): An Overview*, by Patricia Moloney Figliola.

[56] *hiQ Labs*, 31 F.4th at 1195.

[57] *Id.*

[58] 18 U.S.C. § 1030.

[59] *Id.* § 1030(a)(2).

[60] *See generally id.* § 1030.

While the CFAA repeatedly uses the phrases "exceeds authorized access" and "without authorization," the statute does not fully define either phrase.[61] In fact, the statute offers no definition for "without authorization."[62] The CFAA does explain that "exceeds authorized access" means "access[ing] a computer *with authorization* and us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter," but that definition hinges on the meaning of the undefined phrase "with authorization."[63]

On a more fundamental level, the meaning of *authorization*—the common concept in "exceeds authorized access" and "without authorization"—is also undefined by the CFAA.[64] As a result, case law is still developing with respect to what it means to be an authorized computer user.

In *hiQ Labs, Inc. v. LinkedIn Corp.*, the Ninth Circuit[65] suggested that authorization depends on the computer systems at issue and described three categories.[66] The first category encompasses computers where authorization is not required for access in the first place.[67] For example, the Ninth Circuit said that computers that are "open to the general public" to access fall in this category.[68] The category potentially includes servers for publicly accessible websites, since a "defining feature of public websites is that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser."[69] The second category is comprised of computers "for which authorization is required and has been given."[70] This category might include, for example, scenarios where an employer provides an employee with password credentials to enter a company computer.[71] Third, there are computers or areas of computer systems "for which authorization is required but has not been given."[72]

The third category poses a crucial question: in what way must the owner of a computer restrict access so that authorization is *not* given?[73] Federal case law on this question is unresolved. In the 2021 opinion *Van Buren v. United States*, which marked the Supreme Court's first significant foray into the CFAA, the Court described limits on authorization as "gates."[74] The *Van Buren* Court explained that assessing authorization under the CFAA is "a gates-up-or-down inquiry" where "one either can or cannot access a computer system, and one either can or cannot access certain areas within the system."[75] *Van Buren* did not define "gate" but seemed to assume that

[61] *Id.*

[62] *Id.* § 1030(e).

[63] *Id.* (emphasis added).

[64] *Id.* § 1030.

[65] 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 Ninth Circuit) refer to the U.S. Court of Appeals for that particular circuit.

[66] 31 F.4th 1180, 1197–98 (9th Cir. 2022).

[67] *Id.*

[68] *Id.*

[69] *Id.* at 1199.

[70] *Id.* at 1198.

[71] A number of CFAA cases involve authorization to access computers by virtue of employment and more specifically address what happens to that authorization when the employment ends. *E.g.*, United States v. Nosal *(Nosal II)*, 844 F.3d, 1024, 1038 (9th Cir. 2016).

[72] *hiQ Labs*, 31 F.4th at 1198.

[73] *See generally* Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1444–60 (2016) (discussing five paradigms for conceptualizing the limits of authorization).

[74] Van Buren v. United States, 141 S. Ct. 1648, 1658 (2021).

[75] *Id.* at 1658–59.

technological limitations[76] such as password requirements constitute a "gate" or limitation on access.[77] In a footnote, however, *Van Buren* left open the possibility that other gates may exist as well, including "limits contained in contracts or policies."[78] Beyond this discussion, the Court left uncertainty as to what means may be used to limit authorization for CFAA purposes.[79] In other words, an unresolved question is what "gates" effectively limit a user's authorization.[80]

However, in many respects, *Van Buren* appears to foreclose imposing CFAA liability for mere violations of Terms of Service agreements (ToS)—contractual restrictions on computer use.[81] The *Van Buren* Court held that the CFAA does not criminalize accessing computers for unauthorized purposes.[82] Thus, to the extent a contractual restriction such as a ToS limits the purposes for which an individual may access information on a computer—such as an employer policy limiting access to a system for business purposes—violating such restrictions would not incur CFAA liability under *Van Buren*.[83]

Delineating the concept of authorization, and its limits, requires reference to the statutory phrases "exceeds authorized access" and "without authorization," which describe when an individual lacks authorization for CFAA purposes.[84] Both phrases are discussed below.

Without Authorization: As noted, the CFAA offers no definition for "without authorization."[85] However, at least in theory, Congress seemingly intended for "without authorization" to apply to outsiders such as hackers,[86] who are "wholly lacking in authority to access or use [the relevant] computer."[87] Federal courts have generally interpreted "without authorization" to refer to

[76] Some observers use the term "code-based" to describe technological limitations, e.g., Bellia *supra*, note 73, 1457, but the Court has used the phrases "code-based" and "technological" interchangeably with respect to limitations on authorization. *Van Buren*, 141 S. Ct. at 1659 n.8.

[77] It questioned only whether other types of gates *beyond* technological limitations may *also* exist. *See Van Buren*, 141 S. Ct. at 1659 n.8 ("For present purposes, we need not address whether this inquiry turns *only* on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." (emphasis added)).

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] Even before *Van Buren*, some federal courts had concluded that the void-for-vagueness doctrine potentially limited CFAA prosecution for mere terms of service violations. *See generally, e.g.*, United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009). Also prior to *Van Buren*, there was an unresolved circuit split over whether the CFAA could impose criminal liability for ToS violations, as a result of conflicting interpretations of the breadth of the phrases "without authorization" and "exceeds authorized access." *Compare, e.g.*, EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access.") *with, e.g.*, United States v. Nosal (*Nosal I*), 676 F.3d 854, 863 (9th Cir. 2012) ("Instead, we hold that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions.").

[82] *Van Buren*, 141 S. Ct. at 1662.

[83] *Id.*

[84] *See, e.g.*, hiQ Labs v. LinkedIn Corp., 938 F.3d 985, 1003 (9th Cir. 2019), *aff'd*, 31 F.4th 1180 (9th Cir. 2022) (exploring limits of authorization based on whether use of a computer fell into the "without authorization" category as a result of a cease and desist letter).

[85] *Id.* § 1030(e).

[86] S. REP. No. 104-357, at 9 (1996) (describing "outsiders" as those "who gain access to a computer without authorization").

[87] S. REP. No. 99-432, at 8 (1986).

outsiders,[88] and the Supreme Court appears to have approved of that conclusion in its 2021 opinion in *Van Buren v. United States*.[89]

Following *Van Buren*, a number of federal courts have examined what "gates" may cause someone to be without authorization to access a computer. In *hiQ Labs, Inc. v. LinkedIn Corp.*, the Ninth Circuit concluded that "the CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer."[90] Thus, the Ninth Circuit held that an entity was not without authorization in violation of the CFAA when it scraped data from a publicly-accessible website despite a cease and desist letter.[91] The court further held that "the concept of 'without authorization' does not apply to public websites" in general.[92] Using *Van Buren*'s "gates" metaphor for limits on authorization, the Ninth Circuit explained that with respect to a "computer hosting publicly available webpages, that computer has erected no gates to lift or lower in the first place."[93] According to the Ninth Circuit, "[w]ith regard to websites made freely accessible on the Internet . . . the concept of 'without authorization' is inapt."[94]

Some federal district courts appear to have embraced a less restrictive interpretation of "without authorization" than the Ninth Circuit.[95] For instance, one court examined *Van Buren* and rejected the assertion that "hacking a password is the *only* way that one can obtain access 'without authorization.'"[96] That court concluded that a reasonable jury could determine that an individual is "without authorization" when he accesses a webpage that is not password protected, but that he believes was intended to be "password protected based on the obviously sensitive nature of the information" on the page, and when he gained access by "guessing their likely URLs."[97] In an unpublished opinion, one federal district court also concluded that an individual can be without authorization if he accessed a computer in violation of ToS and multiple cease and desist letters.[98] Subsequent to *Van Buren*, at least one federal district court has concluded that termination of

[88] *See, e.g.*, Sandvig v. Barr, 451 F. Supp. 3d 73, 86 (D.D.C. 2020) (collecting case law concluding that "without authorization" encompasses individuals lacking any approval to access a computer, such as outside hackers); Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) ("[A] person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question." (quoting LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)) (emphasis omitted)).

[89] 141 S. Ct. 1648, 1658 (2021) (indicating that a view of "without authorization" that "protects computers themselves by targeting so-called outside hackers" lacking any permission to access a computer "makes sense"); *see also* United States v. Eddings, No. 5:19-CR-00535, 2021 WL 2527966, at *4 (E.D. Pa. June 21, 2021) (characterizing *Van Buren* as agreeing that "without authorization" protects computers from outside hackers).

[90] 31 F.4th 1180, 1201 (9th Cir. 2022).

[91] *Id.*

[92] *Id.* at 1199.

[93] *Id.*

[94] *Id.* at 1198.

[95] *But see, e.g.*, Meta Platforms, Inc. v. BrandTotal Ltd., 605 F. Supp. 3d 1218, 1262 (N.D. Cal 2022) (quoting *hiQ Labs* and holding that "where a website is made available to the public without any authentication requirement in at least the first instance," the phrase "without authorization" is inapplicable, "even if the owner employs technological measures to block specific users, suspicious activity, or—as here—repeated access beyond a particular threshold").

[96] Vox Mktg. Grp. v. Prodigy Promos, 556 F. Supp. 3d 1280, 1285 (D. Utah 2021)

[97] *Id.* at 1287.

[98] ACI Payments, Inc. v. Conservice, LLC, No. 1:21-CV-00084-RJS-CMR, 2022 WL 622214, at *9 (D. Utah Mar. 3, 2022).

employment may revoke authorization and leave the former employee without authorization to access a computer previously accessed by virtue of that employment.[99]

Exceeds Authorized Access: The meaning of the phrase "exceeds authorized access" long divided federal courts.[100] Prior to *Van Buren*, some federal appellate courts, including the First,[101] Fifth,[102] Seventh,[103] and Eleventh[104] Circuits, had adopted a broad view of the CFAA where "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'"[105] In contrast, several other courts, including the Second,[106] Fourth,[107] and Ninth[108] Circuits, had more narrowly interpreted "exceeds authorized access," based on an understanding that the CFAA's central purpose is to criminalize hacking. These courts applied CFAA liability only to those who lacked any authorization to access a computer or website[109] or who were "authorized to access only certain data or files" but accessed "unauthorized data or files."[110]

In *Van Buren*, the Court appears to have interpreted the CFAA's scope in a manner roughly consistent with courts that had applied a narrow interpretation of the statute—reading "exceeds authorized access" to exclude an individual who uses a computer for an inappropriate reason.[111] The *Van Buren* court concluded that a police officer did not exceed authorized access when he used a law enforcement database, which he was authorized to use "only for law enforcement purposes," to search for license plate information for personal profit.[112] Thus, pursuant to *Van Buren*, in order to "exceed authorized access" in violation of the CFAA, an individual must access an area of a computer or information on a computer that is completely "off limits to him," as

[99] *See* Zap Cellular, Inc. v. Weintraub, No. 15-CV-6723-PKC-VMS, 2022 WL 4325746, at *7 (E.D.N.Y. Sept. 19, 2022) (distinguishing *Van Buren* and concluding that termination of CEO made him without authorization to access computers and servers he was previously able to access only through his prior employment).

[100] Van Buren v. United States, 210 L. Ed. 2d 26, 141 S. Ct. 1648, 1654 (2021) (referencing "split in authority regarding the scope of liability under the CFAA's 'exceeds authorized access' clause").

[101] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access.").

[102] United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (holding that authorized access may "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 crime").

[103] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (concluding that defendant lacked authorization after breaching duty of loyalty to employer).

[104] 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).

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

[106] 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).

[107] WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) ("[W]e adopt a narrow reading of the terms 'without authorization' and 'exceeds authorized access' and hold that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access.").

[108] United States v. Nosal (*Nosal I*), 676 F.3d 854, 863 (9th Cir. 2012) ("Instead, we hold that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions.").

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

[110] *Nosal I*, 676 F.3d at 856–57.

[111] Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

[112] *Id.* at 1652.

opposed to accessing a computer or information that he is entitled to use in at least some circumstances.[113]

Damage

The CFAA defines "damage" to mean "impairment to the integrity or availability of data, a program, a system, or information,"[114] which occurs, for example, when a hacker causes a computer to behave in a manner contrary to the intentions of its owner.[115] Thus, an act that causes damage under the CFAA may include "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 email account."[116] For example, one federal court concluded that damage occurred as a result of an orchestrated effort to bombard a company's "sales offices and three of its executives with thousands of phone calls and e-mails," which diminished the ability of that company to use their systems.[117]

Prohibited Conduct Under the CFAA

The CFAA prohibits seven categories of conduct, ranging from certain acts of computer trespass to unauthorized computer access with an intent to defraud.[118]

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

Section 1030(a)(1)[119] is a cyber-espionage provision that in certain instances prohibits obtaining and sharing national security information[120]—such as "information that has been determined by

---

[113] *Id.* at 1662.

[114] 18 U.S.C. § 1030(e)(8).

[115] *See* CRS Legal Sidebar LSB10446, *An Overview of Federal Criminal Laws Implicated by the COVID-19 Pandemic*, by Peter G. Berris at 2 (explaining that damage "occurs, for example, where a hacker causes a computer to behave in a manner contrary to the intentions of its owner"); *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 computer is caused to "no longer operate[] only in response to the commands of the owner"); *see also* United States v. Hutchins, 361 F. Supp. 3d 779, 794 (E.D. Wis. 2019) (concluding that use of the phrase "malware" in indictment was "sufficient to allege intent to cause damage" in CFAA prosecution). For a more detailed examination of different examples of damage, see, e.g., KERR, *supra* note 12 at 113–15.

[116] *Hutchins*, 361 F. Supp. 3d at 794 (alterations in original) (quoting Fidlar Tech. v. LPS Real Estate Data Sols., Inc., 810 F.3d 1075, 1084–85 (7th Cir. 2016)).

[117] Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d, 295, 299 (6th Cir. 2011).

[118] 18 U.S.C. § 1030.

[119] 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.

[120] Certain elements of a § 1030(a)(1) violation may be found in other federal espionage laws such as the willful (continued...)

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.... "[121] According to DOJ, examples of national security information under § 1030(a)(1) could include "classified information obtained from a Department of Defense computer or restricted data obtained from a Department of Energy computer."[122] In practice, the provision has been rarely invoked, if at all,[123] perhaps because prosecutors may charge offenses involving national security information under federal espionage statutes that overlap with § 1030(a)(1).[124]

Prosecutions under § 1030(a)(1) require the government to establish several elements beyond a reasonable doubt. First, the government would need to prove that the defendant obtained the national security information by knowingly[125] accessing a computer without authorization or in excess of authorization.[126] Section 1030(a)(1) broadly covers all computers, as opposed to just protected computers[127]—for example, those exclusively used by financial institutions or connected to the internet.[128] Second, a § 1030(a)(1) violation requires the government to establish that the defendant had reason to believe that the information could cause "injury to the United States" or benefit "any foreign nation."[129] There is little case law expounding on this element, but DOJ has indicated that the element can likely be satisfied where "the national security information is classified or restricted" and the defendant was aware of that fact.[130] Finally, the government must prove that the defendant "willfully communicate[d], deliver[ed], transmit[ted] or ... retain[ed]" the national security information, or attempted to do so, or caused the communication, delivery, or transmission of national security information.[131] This element is broad, and by its own terms includes a range of activities including the failure to return national

disclosure of covered classified information. *E.g.*, 18 U.S.C. §§ 793, 794, 798; *see also* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 14–16 (comparing § 1030(a)(1) to various espionage laws).

[121] 18 U.S.C. § 1030(a)(1).

[122] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 13.

[123] *See* KERR, *supra* note 12, at 30 ("Although it is the first in the list of § 1030(a) crimes, [§ 1030(a)(1)] appears never to have been used.").

[124] *See, e.g.*, Press Release, U.S. Dep't of Just., 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 Department of Defense "classified systems," which defendant "had no need to access," and transmitting that information to "a foreign terrorist organization"); *accord* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 15 ("In situations where both [§ 1030(a)(1) and a federal espionage statute] ... are applicable, prosecutors may tend towards using [the espionage statutes], for which guidance and precedent are more prevalent.").

[125] Although the CFAA does not define "knowingly," and despite a dearth of case law on § 1030(a)(1), a Senate report accompanying the 1986 amendment to the CFAA noted that a knowing act is one where the person is aware "that the result is practically certain to follow from his conduct, whatever his desire may be as to that result." S. REP. NO. 99-432, 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 that § 1030(a)(5)(A) requires showing that "defendant intended to cause harm" and that "[d]amage caused by mere recklessness or negligence is insufficient").

[126] 18 U.S.C. § 1030(a)(1).

[127] *Id.*

[128] *See supra* Section "Protected Computers."

[129] 18 U.S.C. § 1030(a)(1).

[130] U.S. DEP'T OF JUST., *supra* note footnote 12, at 14.

[131] 18 U.S.C. § 1030(a)(1).

security information or the disclosure of that information.[132] However, such behavior must be intentional.[133]

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

Section 1030(a)(2)[134] generally prohibits accessing a computer without authorization or in excess of authorization and obtaining information in certain circumstances. Although at first glance, it could appear that to "obtain information" might refer specifically to misappropriation or theft of information, the concept is much broader.[135] As interpreted by courts, "obtaining information" includes "mere observation of the data" such as looking at or reading information on a screen.[136] The government has invoked § 1030(a)(2) in a variety of prosecutions,[137] including in the case of several individuals for "breaking into computer networks of prominent technology companies and the U.S. Army" and stealing "more than $100 million in intellectual property,"[138] two Massachusetts men for stealing social media accounts and cryptocurrency through unauthorized computer access,[139] and an Italian citizen for "hack[ing] into thousands of computers without permission [and] ... gaining access to all of the information stored on those computers."[140]

There are three additional statutory requirements that the government must satisfy to prove a § 1030(a)(2) violation—only one of which seems to limit the provision's scope in a significant

---

[132] *Id.*

[133] *Id.*

[134] 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.

[135] *See* United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009) ("'Obtain[ing] information from a computer' has been described as 'includ[ing] mere observation of the data. Actual aspiration ... need not be proved in order to establish a violation.... '" (alterations in original) (quoting S. REP. NO. 99-432, at 6–7 (1986))); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000) (relying on legislative history for the proposition that § 1030(a)(2) covers not just theft but also the observation of data).

[136] *See Drew*, 259 F.R.D. at 457 n.13 ("[T]he term 'obtaining information' includes merely reading it." (alteration in original) (quoting S. REP. NO. 104–357, at 7 (1996))).

[137] Section 1030(a)(2) is "the most commonly charged section of the [CFAA]." KERR, *supra* note 12, at 79.

[138] Press Release, U.S. Dep't of Just., Four Members of International Computer Hacking Ring Indicted for Stealing Gaming Technology, Apache Helicopter Training Software (Sept. 30, 2014), https://www.justice.gov/opa/pr/four-members-international-computer-hacking-ring-indicted-stealing-gaming-technology-apache; Memorandum of Plea Agreement, United States v. Leroux, No. 13-78-GMS, 2015 WL 10372423 (D. Del. Jan. 20, 2015) (setting forth plea of guilty to conspiracy to violate § 1030(a)(2)).

[139] Press Release, U.S. Dep't of Just., Two Massachusetts Men Arrested and Charged with Nationwide Scheme to Steal Social Media Accounts and Cryptocurrency (Nov. 14, 2019), https://www.justice.gov/opa/pr/two-massachusetts-men-arrested-and-charged-nationwide-scheme-steal-social-media-accounts-and; Press Release, U.S. Dep't of Just., Massachusetts Man Pleads Guilty to Operating Nationwide Scheme to Steal Social Media Accounts and Cryptocurrency (Apr. 28, 2021), https://www.justice.gov/opa/pr/massachusetts-man-pleads-guilty-operating-nationwide-scheme-steal-social-media-accounts-and; Indictment, United States v. Meiggs, No. 19-CR-10438, 2019 WL 12117167 (D. Mass. Nov. 13, 2019).

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

way.[141] First, for § 1030(a)(2) to apply, the information must be obtained from either a financial institution,[142] the federal government, or "any protected computer."[143] As discussed, any computer connected to the internet suffices. Second, § 1030(a)(2) requires intentional access to a computer by the defendant, "rather than mistaken, inadvertent, or careless" access.[144] However, the intent requirement is a low bar to prosecution because intent to obtain information is not required; instead, all that is required is intent to access a computer without authorization or in excess of authorization.[145] Third, the defendant's access must be without authorization or in excess of authorization—elements that are discussed above. Before *Van Buren*, this requirement arguably did little to limit the expansive scope of § 1030(a)(2), at least in jurisdictions that had adopted a broad interpretation of the phrase "exceeds authorized access."[146] However, by limiting "exceeds authorized access" to exclude an individual who uses a computer for an unapproved reason, *Van Buren* solidified the element as a more meaningful limit on § 1030(a)(2) prosecutions.[147] As discussed, *Van Buren* reversed a § 1030(a)(2) conviction on these grounds—concluding that a police officer who was authorized to access information from a law enforcement database for official purposes only, did not exceed authorized access in violation of § 1030(a)(2) by accessing information from that database for other purposes.[148]

Government Computer Trespassing, 18 U.S.C. § 1030(a)(3)

Section 1030(a)(3)[149] generally prohibits intentionally accessing a government computer without authorization. The provision establishes "a simple trespass offense,"[150] which at common law often refers to an unsanctioned entry onto the land of another, regardless of whether that entry causes any harm.[151] Unlike the previous two CFAA prohibitions, the crux of a § 1030(a)(3)

---

[141] *See generally* KERR, *supra* note 12, at 81–82 (explaining breadth of § 1030(a)(2) and why requirements in that provision pose "relatively low thresholds").

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

[143] 18 U.S.C. § 1030(a)(2).

[144] S. REP. NO. 99-432, at 5 (1986).

[145] United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007) ("A plain reading of the statute reveals that the requisite intent to prove a violation of § 1030(a)(2)(C) is ... intent to obtain unauthorized access of a protected computer.... The government need not also prove that the defendant had the intent to defraud in obtaining the information or that the information was used to any particular ends."); United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) ("The only scienter element in section 1030(a)(2)(C) is the requirement that the person must 'intentionally' access a computer without authorization or 'intentionally' exceed authorized access.").

[146] As one court described the pre-*Van Buren* landscape, barring a narrow interpretation of "without authorization" or "exceeds authorized access," it was possible that § 1030(a)(2) could criminalize any conscious violation of ToS or other contractual restrictions on computer use. *Drew*, 259 F.R.D. at 457.

[147] Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

[148] *Id.* at 1652.

[149] 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.

[150] S. REP. NO. 99-432, at 7 (1986) (clarifying that § 1030(a)(3) "applies to acts of simple trespass against computers belonging to, or being used by or for, the Federal Government").

[151] *E.g.*, Restatement (Second) of Torts § 158 (1965). Criminal liability for trespass—under various statutes—often (continued...)

violation is unauthorized entry into a government computer, and the provision does not require that the defendant do anything with, or obtain anything from, the covered computer once he has accessed it.[152] The provision is seldom invoked by prosecutors, possibly because it overlaps significantly with § 1030(a)(2), which imposes stricter penalties.[153]

There are two ways the government can establish a § 1030(a)(3) violation.[154] First, the government may demonstrate that the defendant accessed a "nonpublic computer of a department or agency of the United States" used *exclusively* by the federal government.[155] A nonpublic computer includes one for internal use, such as the data servers of a federal agency.[156] The term nonpublic computer excludes, however, public-facing government computers, internet servers, and websites, such as those offering public services or information.[157] Second, the government may establish a § 1030(a)(3) violation where the defendant accesses a "nonpublic computer of a department or agency of the United States," if that computer is used *in part* by the federal government and the defendant's "conduct affects that use."[158] A computer used in part by the federal government might include, for example, a private company's computer on which the federal government has an account.[159] In practice, "[a]lmost any network intrusion will affect the government's use of its computers because any intrusion potentially affects the confidentiality and integrity of the government's network and often requires substantial measures to assure the integrity of data and the security of the network."[160]

Regardless of the nature of the § 1030(a)(3) violation, the government must prove that the defendant's access was intentional and without authorization.[161] The intent requirement is identical to the one in § 1030(a)(2). Although the meaning of "without authorization" is also discussed above,[162] it is notable that the statute excludes liability where the defendant's conduct merely exceeds authorized access.[163] Based on legislative history, it appears that such language

involves additional requirements such as notice to a person that he is trespassing, followed by that person's knowing refusal to vacate the area in which he is trespassing. *E.g.*, CONN. GEN. STAT. § 53a-107.

[152] *See* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 23 ("Section 1030(a)(3) protects against 'trespasses' by outsiders into federal government computers, even when no information is obtained during such trespasses."); S. REP. 99-432 at 7 (1986) (explaining that with amendment, § 1030(a)(3) will apply "to acts of simple trespass against computers belonging to, or being used by or for, the Federal Government"); *see also* H.R. REP. 99-612 at 11 (1986).

[153] *See* U.S. DEP'T OF JUST., *supra* note 36, at 25 (explaining why § 1030(a)(2) may be the "preferred charge" in instances where both § 1030(a)(2) and § 1030(a)(3) could apply).

[154] 18 U.S.C. § 1030(a)(3).

[155] *Id.*

[156] *See* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 24 ("'Nonpublic' includes most government computers, but not Internet servers that, by design, offer services to members of the general public.").

[157] *Id.*

[158] 18 U.S.C. § 1030(a)(3).

[159] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 24.

[160] *Id.*; *see also* Sawyer v. Dep't of Air Force, 31 M.S.P.R. 193, 196 (1986) ("The elements for establishing a criminal 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 unauthorized purpose.").

[161] 18 U.S.C. § 1030(a)(3).

[162] *See supra* Section "Without Authorization and Exceeds Authorized Access."

[163] 18 U.S.C. § 1030(a)(3).

was omitted to foreclose criminal liability against those who have some authorization, like federal employees approved to use a government computer, but who do so in an unapproved manner.[164]

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

Section 1030(a)(4)[165] is an anti-fraud provision, which makes it a crime to "knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access" and obtain anything of value, or obtain use of the computer itself if that use is worth at least $5,000 a year.[166] Prosecutors have used § 1030(a)(4) to charge a variety of fraudulent activities involving computers, including the use of a lottery terminal to falsely generate winning tickets,[167] a phishing scheme that netted "hundreds of thousands of dollars,"[168] and a plot to use misappropriated computer credentials to inflate grades at two universities.[169]

To prove a violation of § 1030(a)(4), the government must first establish that the defendant "knowingly and with intent to defraud, access[ed] a protected computer without authorization, or exceed[ed] authorized access."[170] The statute does not define what it means to act knowingly and with intent to defraud in the context of § 1030(a)(4).[171] However, in the context of a civil § 1030(a)(4) claim, one federal court has indicated that "intent to defraud" means to act "willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for one's self or causing financial loss to another."[172] Further guidance on the meaning of "knowingly and with intent to defraud" may be found in the legislative history of § 1030(a)(4), which notes that the identical standard is also employed in 18 U.S.C. § 1029 (governing credit card fraud).[173]

---

[164] 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 (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 protect Government computers against abuse by "outsiders."

[165] 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.

[166] *Id.*

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

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

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

[170] 18 U.S.C. § 1030(a)(4).

[171] *Id.* § 1030(e); Good 'Nuff Garage, LLC v. McCulley, No. 3:21CV571, 2022 WL 4485810, at *14 (E.D. Va. Sept. 26, 2022); *see also* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 27 ("The phrase 'knowingly and with intent to defraud' is not defined by 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 the phrase.").

[172] 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)), *aff'd*, 810 F.3d 1075 (7th Cir. 2016); *see also* United States v. Nosal *(Nosal I)*, 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 have concluded that to "defraud" under § 1030(a)(4) refers 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) ("The term 'defraud' for purposes of § 1030(a)(4) simply means wrongdoing and does not require proof of common law fraud.").

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

In the context of § 1029, at least one federal appellate court has concluded that § 1029 requires proof of the defendant's "intent to deceive and cheat, which means the government must prove that the defendant had the intent to deprive a victim of money or property by deception."[174]

There are two additional requirements for violations of § 1030(a)(4). First, the government must prove that in accessing the protected computer, the defendant furthered the fraud.[175] In other words, the access must be "directly linked to the intended fraud."[176] Thus, § 1030(a)(4) does not govern frauds where the computer use is incidental—for example, where an individual simply uses the computer for record keeping or to "add up his potential 'take' from the [fraud]."[177] Second, the government must prove that the defendant obtained "anything of value."[178] That element is "easily met if the defendant obtained money, cash, or a good or service with measurable value."[179] One "typical item of value" is data,[180] but merely viewing information may not suffice on its own.[181] Rather, as at least one court has concluded, the information must be valuable not merely in the abstract, but specifically to the defendant "in light of a fraudulent scheme."[182] Thus, information may not be a thing of value when viewed only to "satisfy idle curiosity."[183]

Computer use, in and of itself, also may be a thing of value for the purposes of § 1030(a)(4), but only if that use is worth at least $5,000 a year.[184] The concept of computer use as a thing of value is underdeveloped in case law, but 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.[185] Although at least one observer has suggested that this idea is outmoded given the modern prevalence of computers and the corresponding decrease in the value of computer use,[186] 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.[187] In any event, the $5,000 threshold for fraud solely resulting in computer use is intended to prevent § 1030(a)(4) from encompassing mere computer trespass in most cases.[188] As the same 1986 Senate report observed, if every trespass were thought of as "an attempt to defraud a service provider of

[174] United States v. Saini, 23 F.4th 1155, 1160 (9th Cir. 2022) (emphasis omitted).

[175] 18 U.S.C. § 1030(a)(4).

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

[177] *Id.*

[178] 18 U.S.C. § 1030(a)(4).

[179] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 32.

[180] *In re* Am. Online, Inc., 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001).

[181] United States v. Czubinski, 106 F.3d 1069, 1078–79 (1st Cir. 1997) (reversing defendant's § 1030(a)(4) conviction for obtaining information where the "evidence did not show that [defendant's] end was anything more than to satisfy his curiosity," because the "[t]he value of information is relative to one's needs and objectives" and "the government had to show that the information was valuable to [the defendant] in light of a fraudulent scheme").

[182] *Id.* at 1078.

[183] *Id.*

[184] 18 U.S.C. § 1030(a)(4).

[185] S. REP. NO. 99-432, at 10 (1986) ("The Committee agrees that the mere use of a computer or computer service has a value all its own. Mere trespasses onto someone else's computer system can cost the system provider a 'port' or access channel that he might otherwise be making available for a fee to an authorized user.").

[186] KERR, *supra* note 12, at 102–03.

[187] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 32.

[188] *See Czubinski*, 106 F.3d at 1078 (reviewing legislative history supporting conclusion that "Congress intended section 1030(a)(4) to punish attempts to steal valuable data, and did not wish to punish mere unauthorized access").

computer time," it would obliterate the distinction between § 1030(a)(4) and the CFAA provisions that prohibit trespass.[189] 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.[190] Rather, for at least one federal court, unauthorized access must be coupled with "the showing of some additional end—to which the unauthorized access is a means."[191]

Damaging a Computer, 18 U.S.C. § 1030(a)(5)

Broadly speaking, § 1030(a)(5)[192] prohibits a variety of acts that result in damage to a computer, including:

- knowingly causing the transmission of "a program, information, code, or command," and thereby "intentionally caus[ing] damage without authorization to a protected computer;" and
- intentionally accessing a protected computer without authorization, and thereby:
  - recklessly causing damage, or
  - causing damage or loss.

Subsection 1030(a)(5) may be used to prosecute many of the activities that are commonly associated with hacking, such as the transmission of viruses or worms[193] and unauthorized access by intruders who delete files or shut off computers.[194] The provision may also be used to prosecute the perpetrators of Distributed Denial of Service (DDoS) attacks,[195] which occur, for example, when an attacker overwhelms a server's ability to process legitimate requests by overloading the server with a flood of illegitimate traffic.[196] The government has invoked § 1030(a)(5) in a variety of prosecutions, such as those of a Russian national for deploying malware

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

[190] *Czubinski*, 106. F3d at 1075 (concluding that government did not adequately prove "intent to deprive ... and, *a fortiori*, a scheme to defraud" where defendant accessed computer and looked at confidential information, but there was no evidence that defendant intended to use that information for anything other than browsing).

[191] *Id.* at 1078.

[192] 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.

[193] "In the colorful argot of computers, a 'worm' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects.' It differs from a 'virus,' which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer." United States v. Morris, 928 F.2d 504, 505 n.1 (2d Cir. 1991).

[194] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 35.

[195] *E.g.*, United States v. Gottesfeld, 18 F.4th 1, 4 (1st Cir. 2021), *cert. denied*, 143 S. Ct. 85 (2022) (affirming § 1030(a)(5) conviction of defendant for a DDoS attack he committed against Boston Children's Hospital and Wayside Youth and Family Support Network).

[196] *Understanding Denial-of-Service Attacks*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Feb. 01, 2021), https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.

that "resulted in tens of millions of dollars of losses to victims worldwide";[197] an Illinois resident for developing websites used to launch "millions of DDoS attacks that disrupted the internet connections of targeted victim computers";[198] and the former IT employee of a major railroad who damaged his employer's computer network by "strategically delet[ing] files, remov[ing] administrative-level accounts, and chang[ing] passwords."[199] Section 1030(a)(5) has also been used to prosecute the *developers* and *purveyors* of malware, such as ransomware, often in conjunction with inchoate offenses like conspiracy and aiding and abetting.[200]

The first act that § 1030(a)(5) criminalizes—specifically, under subsection (A)—is to "knowingly cause[] the transmission of a program, information, code, or command" and thereby "intentionally cause[] damage without authorization, to a protected computer."[201] The CFAA does not define "transmission,"[202] but the phrase likely "encompasses a range of hacking activities, such as '[t]he transfer of operational or confidential information,' 'malicious software updates,' 'code injection attacks,' DDoS, and the 'embedding of malicious code' or malware."[203] Transmission may occur through use of the internet or physical media like compact discs.[204]

---

[197] Press Release, U.S. Dep't of Just., 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 Deployment of "Bugat" Malware (Dec. 5, 2019), 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).

[198] Press Release, U.S. Dep't of Just., 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.

[199] Press Release, U.S. Dep't of Just., Former IT Employee of Transcontinental Railroad Sentenced to Prison for Damaging Ex-Employer's Computer Network (Feb. 13, 2018), https://www.justice.gov/opa/pr/former-it-employee-transcontinental-railroad-sentenced-prison-damaging-ex-employer-s-computer.

[200] For instance, prosecutors charged a member of a North Korean hacking team for conspiracy to violate CFAA provisions such as § 1030(a)(5) in connection with a scheme that involved developing the ransomware known as WannaCry2.0. Press Release, U.S. Dep't of Just., North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and; Criminal Complaint, United States v. Park Jin Hyok, No. MJ18-1479 (C.D. Cal. June 8, 2018). As another example, federal prosecutors charged one individual under § 1030(a)(5), among other things, in connection with his "creation and distribution of the Kronos banking Trojan and UPAS kit malware." Press Release, U.S. Dep't of Just., 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; First Superseding Indictment, United States v. Hutchins, No. 2:17-CR-00124, 2018 WL 7325296 (E.D. Wis. June 5, 2018). Prosecutors also used § 1030(a)(5), along with other provisions, to charge a Swedish national responsible for the sale of malware to "thousands of people in more than 100 countries." Press Release, U.S. Dep't of Just., Swedish Co-Creator Of "Blackshades" Malware That Enabled Users Around The World To Secretly And Remotely Control Victims' Computers Sentenced To 57 Months In Prison (June 23, 2015), https://www.justice.gov/usao-sdny/pr/swedish-co-creator-blackshades-malware-enabled-users-around-world-secretly-and-remotely; United States v. Yücel, 97 F. Supp. 3d 413, 416 (S.D.N.Y. 2015).

[201] 18 U.S.C. § 1030(a)(5)(A).

[202] Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1034 (N.D. Ill. 2008).

[203] Beale & Berris, *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)); *see also* Lloyd v. United States, No. CIV.03-813(WHW), 2005 WL 2009890, at *7–*8 (D.N.J. Aug. 16, 2005) (discussing the breadth of "transmission" under CFAA).

[204] Meridian Fin. Advisors, Ltd. v. Pence, 763 F. Supp. 2d 1046, 1061 (S.D. Ind. 2011); *see also* United States v. Sullivan, 40 F. App'x 740, 743–44 (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. 19, 1996) ("The transmission of a disabling code by floppy computer disk may fall within ... [§ 1030(a)(5)(A)], if accompanied by the intent to cause harm.").

Some courts have gone so far as to conclude that the exact means of transmission is irrelevant, focusing instead on whether the program, information, code, or command caused damage.[205] The CFAA also does not define the phrase "program, information, code, or command."[206] The phrase seemingly includes "all transmissions that are capable of having an effect on a computer's operation," such as worms, "software commands (such as an instruction to delete information)," and "network packets designed to flood a network connection or exploit system vulnerabilities."[207]

To prove a § 1030(a)(5)(A) violation, the government must establish dual mental states on the part of the defendant. First, the government must prove that the defendant's transmission was knowing.[208] The CFAA does not define "knowing,"[209] but it almost certainly excludes accidental transmission—for example, in the case of an unsuspecting user who forwards an email with malware attached in a file or link.[210] Second, the government must prove that the defendant intentionally caused damage to a protected computer without authorization.[211] The meanings of "protected computer," "without authorization," and "damage" are discussed in detail above. According to at least one court, the requirement of intent to cause damage in the context of § 1030(a)(5)(A) means that the defendant had the "conscious purpose of causing damage ... to [the relevant] computer."[212]

Other violations of § 1030(a)(5) may occur where a defendant intentionally accesses a protected computer without authorization and causes damage, even if he does *not* intend to cause such damage.[213] However, for such unintended damage to amount to a § 1030(a)(5) violation, it must either be reckless or result in loss.[214] Although the CFAA does not define what it means to recklessly cause damage, in general the "normal meaning of reckless in the criminal law (unlike

[205] *See, e.g.*, *Patrick Patterson Custom Homes*, 586 F. Supp. 2d at 1035 ("While 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 irrelevant.").

[206] 18 U.S.C. § 1030(e).

[207] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 37; *see also* United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991) (affirming § 1030(a)(5)(A) conviction of defendant who created and released a worm); Arience Builders, Inc. v. Baltes, 563 F. Supp. 2d 883, 884 (N.D. Ill. 2008) (discussing when instructions to delete information may amount to transmission of a command for CFAA purposes).

[208] 18 U.S.C. § 1030(a)(5)(A).

[209] *Id.* § 1030(e).

[210] For example, in the context of another federal criminal statute, one federal appellate court approved of jury instructions that conduct is undertaken "knowingly" when "the defendant realized what he was doing and was aware of the nature of his conduct, and did not act through ignorance, mistake or accident." United States v. Salinas, 763 F.3d 869, 879 (7th Cir. 2014); *see also* Good 'Nuff Garage, LLC v. McCulley, No. 3:21CV571, 2022 WL 4485810, at *14 (E.D. Va. Sept. 26, 2022) (discussing use of "knowingly" in another CFAA provision and explaining that "in the criminal context, 'knowingly' is often interpreted to mean that a party acted 'voluntarily and intentionally and not because of accident, mistake or some other innocent reason.'" (quoting United States v. Fall, No. 2:17CR12, 2018 WL 9854664, at *2 (E.D. Va. May 14, 2018), *aff'd*, 955 F.3d 363 (4th Cir. 2020))).

[211] 18 U.S.C. § 1030(a)(5)(A).

[212] Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 303 (6th Cir. 2011); *accord* United States v. Carlson, 209 F. App'x 181, 184 (3d Cir. 2006) (discussing § 1030(a)(5) prosecution and noting that although CFAA does not define "intentionally," "this Court has defined it in the criminal context as performing an act deliberately and not by accident"); *see also* QVC, Inc. v. Resultly, LLC, 99 F. Supp. 3d 525, 536 (E.D. Pa. 2015) (concluding that § 1030(a)(5)(A) requires showing that "defendant intended to cause harm" and that "[d]amage caused by mere recklessness or negligence is insufficient").

[213] 18 U.S.C. § 1030(a)(5).

[214] *Id.*

the civil law) is that the defendant disregarded 'a risk of harm of which he is aware.'"[215] Case law specific to the CFAA provides few illustrations, but an individual may recklessly cause damage to a computer if he is aware of the risk that his unauthorized computer access may cause damage and proceeds anyway in a way that does indeed damage the computer.[216] The CFAA defines "loss" as "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."[217] Federal courts disagree on whether proving interruption of service—such as computer systems or files being rendered unavailable—is a prerequisite to demonstrating loss.[218] 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.[219]

Password Trafficking, 18 U.S.C. § 1030(a)(6)

Section 1030(a)(6)[220] is a rarely used[221] provision of the CFAA designed to protect computer passwords.[222] The provision is "aimed at penalizing conduct associated with 'pirate bulletin boards,' where passwords are displayed that permit unauthorized access to others' computers."[223] Specifically, the law, assuming an appropriate jurisdictional nexus discussed below, makes it a crime to traffic "knowingly and with intent to defraud" in "any password or similar information

---

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

[216] 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 the plaintiff's website, accounts, 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).

[217] 18 U.S.C. § 1030(e)(11). For a detailed examination of "loss," see, e.g., KERR, *supra* note 12, at 124–30.

[218] *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).

[219] *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-13582, 2011 WL 3880489, at *4 (E.D. Mich. Sept. 2, 2011) ("The CFAA only covers lost revenue if the loss occurred as a result of interrupted service."), *and* CoStar Realty Info., Inc. v. Field, 737 F. Supp. 2d 496, 515 (D. Md. 2010) ("[A] violation of the CFAA must cause an interruption of service in order for lost revenue to constitute as a qualifying 'loss' under the statute.").

[220] 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.

[221] For example, as of December 27, 2022, a search of the Westlaw database for reported federal cases yielded 33 results that included the phrase "1030(a)(6)," which would be expected in cases discussing that subsection. *See also* AtPac, Inc. v. Aptitude Sols., Inc., 730 F. Supp. 2d 1174, 1182 (E.D. Cal. 2010) ("The court notes that, in the course of its own research, it has come across only a handful of federal cases that even mention § 1030(a)(6).")

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

[223] *Id.*

through which a computer may be accessed without authorization."[224] For the purposes of § 1030(a)(6), "traffic" means to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of."[225] According to at least one court, "trafficking" under § 1030(a)(6) may include the "very common act of giving someone else your password," but such behavior "becomes illegal" only where the other elements of §1030(a)(6) are satisfied and where "the password can enable the password recipient to access a computer without authorization."[226] Based on the definition of "traffic," a defendant must intend to transfer or dispose of the passwords or similar information.[227] "Knowingly with intent to defraud" is the same standard used 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.[228] One federal court concluded that intent to defraud "in the § 1030(a)(6) context requires more than the intent to impermissibly give access to another."[229] Thus, in that case, the court concluded that the act of sharing a password without permission—even if it potentially violated a license agreement—did not "rise to an inference of any 'intent to defraud'" without additional factual allegations of fraud.[230] "Password[s] or similar information"[231] is a broad category intended to include not "only a single word that enables one to access a computer," but also "longer more detailed explanations on how to access others' computers."[232]

For § 1030(a)(6) to apply, the defendant's actions must satisfy one of two jurisdictional hooks. First, § 1030(a)(6) could apply where the "trafficking affects interstate or foreign commerce."[233] 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.[234] For example, for at least one court, trafficking involving the internet could satisfy the requirement.[235] Second, § 1030(a)(6) may also apply where the defendant traffics in passwords or similar information that would allow unauthorized entry into a "computer ... used by or for the Government of the United States."[236] Again there is no statutory definition and little interpretive case law, but according to DOJ the "plain meaning [of the phrase] should encompass any computer used for official business by a federal government employee or on behalf of the federal government."[237] However, it is at least possible that the provision only

[224] 18 U.S.C. § 1030(a)(6).

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

[226] *AtPac, Inc.*, 730 F. Supp. 2d at 1182–83.

[227] 18 U.S.C. §§ 1029(e)(5), 1030(a)(6); *accord* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 50.

[228] *See supra* Section "Computer Fraud, 18 U.S.C. § 1030(a)(4)"

[229] *AtPac, Inc.*, 730 F. Supp. 2d at 1183.

[230] *Id.*

[231] 18 U.S.C. § 1030(a)(6).

[232] S. REP. NO. 99-432, at 13 (1986); *accord* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 50 ("Therefore, prosecutors should apply the term 'password' using a broad meaning to include any instructions that safeguard a computer.").

[233] 18 U.S.C. § 1030(a)(6)(A).

[234] *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).

[235] *Id.* Courts have reached similar conclusions when interpreting 18 U.S.C. § 1029, a credit card fraud statute that prohibits trafficking that "affects interstate or foreign commerce." *See, e.g.*, United States v. Rushdan, 870 F.2d 1509, 1513–14 (9th Cir. 1989) (concluding that federal jurisdiction under § 1029 included "possession of the numbers of out of state credit card accounts").

[236] 18 U.S.C. § 1030(a)(6)(B).

[237] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 51.

applies to passwords for executive branch agencies. That is because unlike other CFAA provisions, § 1030(a)(6) does not specify that a government computer is one used by any "department or agency of the United States"—a phrase that the CFAA specifically defines as including legislative, executive, and judicial branch computers.[238] Thus, the use in § 1030(a)(6) of the phrase "computer.... used by or for the Government of the United States" might be interpreted to have a meaning narrower than the phrase "computer[s] of a department or agency of the United States" used elsewhere in the CFAA.[239]

Threats and Extortion, 18 U.S.C. § 1030(a)(7)

Section 1030(a)(7)[240] prohibits certain extortionate threats concerning a protected computer, such as threats to cause damage to, or disclose confidential information from, a protected computer unless given money or a thing of value.[241] The provision has been described as "a high-tech variation on old fashioned extortion."[242] Although a number of other federal criminal statutes also prohibit extortionate threats, the CFAA's legislative history suggests that Congress's concern in enacting this provision was that other "extortion statutes, which protect against physical injury to person or property, [might not] cover intangible computerized information."[243] In particular, the Senate report accompanying the 1996 Amendment to the CFAA noted concern with threats against computer systems such as "situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key."[244] Prosecutors have invoked § 1030(a)(7) to charge a variety of threats against computer systems themselves, such as ransomware plots that use software to encrypt the victim's computer files (rendering them unavailable) until payment is received to unlock those systems.[245] The government has also relied

[238] 18 U.S.C. § 1030(e)(7) ("[T]he term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments.... ").

[239] Given the lack of interpretive case law, this possibility remains speculative. DOJ has noted that "used by or for the Government of the United States" also appears in § 1030(a)(3) and that the plain meaning of the phrase "should encompass any computer used for official business by a federal government employee or on behalf of the federal government." COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 51. There are differences between the use of the phrase in § 1030(a)(3) and § 1030(a)(6), however. Unlike § 1030(a)(6), the language of § 1030(a)(3) applies only where the unauthorized access is of "any nonpublic computer of *a department or agency of the United States*." 18 U.S.C. § 1030(a)(3) (emphasis added). Thus, § 1030(a)(3) incorporates a phrase defined by the CFAA to include computers of all three branches of government, *supra* note 238, whereas § 1030(a)(6) does not.

[240] 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.

[241] *Id.*

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

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

[244] *Id.*

[245] *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. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, (continued...)

on § 1030(a)(7) to prosecute instances in which computers are not the subject of the threat, but rather the means of extortion. For instance, prosecutors have brought charges under § 1030(a)(7) against a hacker who obtained "sensitive records and information" from victim computers, which he threatened to release unless paid a ransom.[246] As another illustration, federal prosecutors invoked § 1030(a)(7) in charging a former government employee who used stolen passwords to obtain "sexually explicit photographs ... from victims' email and social media accounts," which he "threatened to share ... unless the victims ceded to certain demands."[247]

Section 1030(a)(7) specifically prohibits three categories of extortionate threats. First, the provision criminalizes "threat[s] to cause damage to a protected computer."[248] Threats to cause damage might include threats to "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."[249] Second, § 1030(a)(7) proscribes "threat[s] 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."[250] 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 to a protected computer.[251] For example, an individual may fall within this second category when he threatens to hack into a protected computer and obtain sensitive information.[252] He may also fall within the category if he has already hacked into the computer and obtained the information, and he subsequently threatens to disclose it. This latter category could include double extortion ransomware schemes where an attacker not only uses ransomware but also breaches a computer system, steals sensitive information, and threatens to disclose that information if ransom is not paid.[253] Third, it is a crime under § 1030(a)(7) to issue a "demand or request for money or [an]other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion."[254] An example of this type of threat is the use of ransomware to

Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), 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*, 2018 WL 6798078 (No. 3:18 cr-00704-BRM) (charging defendants under both 18 U.S.C. § 1030(a)(7)(C) and § 1030(a)(5)(A)).

[246] Press Release, U.S. Dep't of Just., Member of "The Dark Overlord" Hacking Group Extradited From United 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).

[247] Press Release, U.S. Dep't of Just., Former 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).

[248] 18 U.S.C. § 1030(a)(7)(A).

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

[250] 18 U.S.C. § 1030(a)(7)(B) (emphasis added).

[251] *Id.*

[252] Indictment, *Ford*, 2015 WL 4980336 (No. 1 15-CR-319).

[253] CRS Report R46932, *Ransomware and Federal Law: Cybercrime and Cybersecurity*, by Peter G. Berris and Jonathan M. Gaffney, at 4.

[254] 18 U.S.C. § 1030(a)(7)(C).

extort payment in exchange for providing the decryption key for the victim's files,[255] and prosecutors have used the subsection to charge such conduct.[256]

There are two important limitations to § 1030(a)(7) as it pertains to all three categories of threats. First, for § 1030(a)(7) to apply, the defendant must have acted "with intent to extort from any person any money or other thing of value."[257] In general, extortion refers to "obtaining something or compelling some action by illegal means, as by force or coercion."[258] In the context of § 1030(a)(7), courts have found the requisite intent to extort where, for example, defendants wrongfully obtained confidential information or credentials and demanded money for their return.[259] However, it may not be necessary to establish "that the defendant actually succeeded in obtaining the money or thing of value, or that the defendant actually intended to carry out the threat made."[260] Second, the defendant must have transmitted the threat "in interstate or foreign commerce"[261]—for example, by transmitting the threat through the internet or between computers in two different states.[262]

Remedies and Penalties

The CFAA authorizes a number of remedies for violations of its various prohibitions. Most obviously, violations of the CFAA provisions discussed above are subject to various criminal penalties of fines and imprisonment.[263] The nature of those penalties varies based on the specific subsection at issue (*see* **Table 1**).[264] For example, the maximum prison term for first-time CFAA offenders is one year under § 1030(a)(3),which governs certain acts of trespassing in government computers,[265] but five years under § 1030(a)(4), which is the main anti-fraud provision in the

[255] Berris & Gaffney, *supra* note 253, at 3.

[256] *See, e.g.*, Indictment, *Savandi*, 2018 WL 6798078 (No. 3:18-cr-00704-BRM); Press Release, U.S. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), 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*, 2018 WL 6798078 (No. 3:18-cr-00704-BRM) (charging defendants under both 18 U.S.C. § 1030(a)(7)(C) and § 1030(a)(5)(A)).

[257] 18 U.S.C. § 1030(a)(7).

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

[259] *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 master access to the plaintiff's domains).

[260] COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 53.

[261] 18 U.S.C. § 1030(a)(7).

[262] *See Inplant Enviro-Sys. 2000 Atlanta, Inc.*, 2015 WL 13297963, at *4 (No. 1:15-CV-0394-LMM) (concluding that plaintiff adequately stated a § 1030(a)(7) violation against defendant who transmitted extortionate communication "in interstate or foreign commerce, as [it was] sent via internet"); *accord* United States v. Kammersell, 196 F.3d 1137, 1139 (10th Cir. 1999) (concluding 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).

[263] 18 U.S.C. § 1030. The CFAA gives the FBI "primary authority to investigate" certain CFAA violations, such as 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* FED. BUREAU OF INVESTIGATION, *The Cyber Threat*, https://www.fbi.gov/investigate/cyber. The Department of Justice prosecutes CFAA violations. *See generally* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., *supra* note 12, at 1-56 (summarizing DOJ interpretation guidance on CFAA prosecutions).

[264] 18 U.S.C. § 1030.

[265] *Id.* § 1030(c)(2)(A).

CFAA.[266] The distinction between first-time and repeat offenses is also relevant in the CFAA (*see* **Table 1**). For instance, under § 1030(a)(1)—which prohibits obtaining and disclosing national security information through unauthorized computer access—a violation is generally subject to a maximum prison term of ten years, a fine, or both.[267] If that violation occurs after another CFAA offense, it is subject to a maximum prison term of twenty years, a fine, or both.[268] Within some CFAA provisions, the relevant penalties also depend on the gravity of the defendant's conduct (*see* **Table 2**; **Table 3**; **Table 4**). For example, under § 1030(a)(2)—prohibiting obtaining information in certain circumstances—the penalties are stiffer if the value of the information obtained is greater than $5,000 (*see* **Table 2**).[269] The CFAA provision prohibiting damage to computers—§ 1030(a)(5)—offers another illustration (*see* **Table 3**; **Table 4**). It authorizes longer prison terms for certain outcomes, such as when a violation results in bodily injury or death.[270] The prison terms covered in this section are the maximum *authorized* by the CFAA for each offense; the sentence actually imposed on a given defendant may be less and is a determination informed by the United States Sentencing Guidelines.[271]

With respect to fines, the amounts will vary based on the corresponding prison term authorized by each CFAA subsection. Unless the underlying statute specifies otherwise, for felonies—violations of statutes authorizing a maximum prison term of more than one year[272]—the default maximum fine level is the greater of $250,000 ($500,000 in the case of organizations) or twice the gain or loss associated with the offense.[273] The default maximum fine level for misdemeanors varies.[274] A federal statute classifies the misdemeanor offenses contained in the CFAA as Class A misdemeanors because they are punishable by up to one year of imprisonment.[275] The default maximum fine level for Class A Misdemeanors not resulting in death is the greater of $100,000 ($200,000 in the case of organizations) or twice the gain or loss associated with the offense.[276]

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

[266] *Id.* § 1030(c)(3)(A).

[267] *Id.* § 1030(c)(1)(A).

[268] *Id.* § 1030(c)(1)(B).

[269] *Id.* § 1030(c)(2)(B).

[270] *Id.* § 1030(c)(4)(E)–(F).

[271] *See generally* CRS Report R41696, *How the Federal Sentencing Guidelines Work: An Overview*, by Charles Doyle.

[272] 18 U.S.C. § 3559(a).

[273] *Id.* § 3571.

[274] *Id.*

[275] *Id.* § 3559(a)(6).

[276] *Id.* § 3571(b)(5), (c)(5), (d).

Section*	Description	First Offense**	Subsequent Offense***
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.

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

Description of Offense Under § 1030(a)(5)(A)	Classification	Sentence
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.

In addition to these criminal penalties, the CFAA also provides a private right of action that permits a person who suffers damage or loss due to a CFAA violation to bring suit against the violator. With a civil CFAA claim, the plaintiff can obtain compensatory damages and injunctive

relief or other equitable relief.[277] However, civil actions are possible only 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.[278] Finally, the CFAA includes forfeiture provisions that authorize government confiscation of property that was used in, or derived from, CFAA violations.[279]

Additional CRS Products on CFAA Issues:

- CRS Report R46932, *Ransomware and Federal Law: Cybercrime and Cybersecurity*, by Peter G. Berris and Jonathan M. Gaffney;
- CRS Report R46829, *Domestic Terrorism: Overview of Federal Criminal Law and Constitutional Issues*, by Peter G. Berris, Michael A. Foster, and Jonathan M. Gaffney;
- CRS Legal Sidebar LSB10616, *Van Buren v. United States: Supreme Court Holds Accessing Information on a Computer for Unauthorized Purposes Not Federal Crime*, by Peter G. Berris;
- CRS Legal Sidebar LSB10446, *An Overview of Federal Criminal Laws Implicated by the COVID-19 Pandemic*, by Peter G. Berris;
- CRS Legal Sidebar LSB10869, *If You Do the Space Crime, You May Do the Space Time*, coordinated by Peter G. Berris.

Other Cybercrimes

The concept of cybercrime may encompass more than the various forms of unauthorized access discussed previously in connection with the CFAA. This report identifies several other types of cybercrime and briefly summarizes applicable federal criminal law.

Data Theft

Cybercriminals who intrude into computers may also steal information from those computers.[280] As described above, such conduct may violate CFAA provisions such as § 1030(a)(2) (prohibiting obtaining information through intentional unauthorized access to a protected computer).[281] Depending on the nature of the stolen information, however, additional federal statutes may

[277] *Id.* § 1030(g).

[278] *Id.* § 1030(c)(4)(A)(i).

[279] *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.

[280] *See, e.g.*, Press Release, U.S. Dep't of Just., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax, (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking (describing scheme in which hackers purportedly stole personal data and trade secrets).

[281] *See supra* Section "Obtaining Information by Unauthorized Computer Access, 18 U.S.C. § 1030(a)(2)."

apply.[282] For example, the Economic Espionage Act (EEA)[283]—authorizes criminal penalties[284] for theft of trade secrets, including intangible "financial, business, scientific, technical, economic, or engineering information," that the owner "has taken reasonable measures to keep ... secret" and that "derives independent economic value" from "not being generally known."[285] With certain limitations, the EEA makes it a crime to steal or misappropriate trade secrets:

- with the intent or knowledge that they "will benefit any foreign government," instrumentality, or agent;[286] or
- for economic benefit, if the trade secrets relate to "a product or service used in or intended for use in interstate or foreign commerce."[287]

Federal prosecutors have used the EEA to charge cybercriminals in connection with high profile incidents such as the Equifax hack.[288]

Additional CRS Products on Data Theft Issues:

- CRS Report R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, by Charles Doyle;
- CRS Report R41404, *Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information*, by Stephen P. Mulligan and Jennifer K. Elsea;
- CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh;
- CRS Legal Sidebar LSB10417, *Red Army Equifax Hackers Indicted*, by Charles Doyle;
- CRS In Focus IF12315, *An Introduction to Trade Secrets Law in the United States*, by Christopher T. Zirpoli.

[282] Espionage statutes protect certain classified material and defense information, for example. *E.g.*, 18 U.S.C. §§ 793, 794, 798.

[283] For additional legal analysis of the EEA, including beyond the cybercrime context, see CRS Report R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, by Charles Doyle; CRS In Focus IF12315, *An Introduction to Trade Secrets Law in the United States*, by Christopher T. Zirpoli.For an example of an EEA prosecution outside the cybercrime context, see, e.g., Press Release, U.S. Dep't of Just., Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets, (July 29, 2019), https://www.justice.gov/opa/pr/texas-man-convicted-conspiracy-commit-theft-trade-secrets (announcing conviction of man for trade secret theft conspiracy for a scheme to obtain synthetic foam technology by "poaching employees from a U.S. company and enticing them to bring technical data to his company" (internal quotation marks omitted)).

[284] For theft of trade secrets for economic benefit, the maximum penalties for individuals are fines, or imprisonment of up to 10 years, or both. 18 U.S.C. §§ 1832(a), 3571. Fines may be the greater of $250,000 or twice the gain or loss associated with the offense. *Id.* §§ 1832(a), 3571. For organizations, the maximum fine is "not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization." *Id.* §§ 1832(b), 3571. For economic espionage (theft of trade secrets to benefit foreign governments/agents/instrumentalities), the maximum penalties are higher; individuals face fines of up to $5,000,000, or up 15 years of imprisonment, or both. *Id.* § 1831(a). Organizations that commit economic espionage "shall be fined not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization." *Id.* § 1831(b).

[285] 18 U.S.C. §§ 1831, 1832, 1839(3).

[286] *Id.* § 1831(a).

[287] *Id.* § 1832(a).

[288] Press Release, U.S. Dep't of Just., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax, (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking; Criminal Indictment, United States v. Wu Zhiyong, No. 1:20-CR-046, 2020 WL 5249460 (N.D.Ga. Jan 28, 2020); *see also* Press Release, U.S. Dep't of Just., U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (detailing indictments of "five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries").

Swatting, Doxing, Cyberstalking, and Cyber Harassment

The proliferation of computers and the internet has created new venues, opportunities, and tools for individuals to engage in stalking and other harassing behaviors.[289] Depending on the circumstances, stalking and harassment in the cyber context could violate a number of federal laws. For example, the federal cyberstalking statute, Section 2261A(2) of Title 18 of the United States Code, imposes criminal penalties[290] for, among other things, using the internet, social media, websites, emails, texts, or other similar technologies[291] to "engage in a course of conduct" that:

- places a person "in reasonable fear of the death of or serious bodily injury" to that person, "an immediate family member," a "spouse or intimate partner," or a person's "pet, service animal, emotional support animal, or horse;" or
- "causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress" to a person, or that person's "immediate family member," or "spouse or intimate partner."[292]

Section 2261A(2) includes two important statutory limitations. First, as indicated, it applies only when the defendant engages in a course of conduct; that is, "a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose."[293] Second, § 2261A(2) requires proof that the defendant intended "to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person."[294]

---

[289] Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, 40 AM. J. TRIAL ADVOC. 41, 41 (2016); *see also* Steven D. Hazelwood & Sarah Koon-Magnin, *Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis*, 7 INT'L J. OF CYBER CRIMINOLOGY 155, 155 (2013) ("[T]he Internet and related technology have also become new mediums for misconduct, in that communications via the Internet can be used to threaten, harass, intimidate, and cause harm to others.").

[290] Section 2261A employs a graduated penalty structure. 18 U.S.C. §§ 2261(b); 2261A. Ordinarily, violations incur fines, or imprisonment of up to five years, or both. 18 U.S.C. §§ 2261(b)(5), 2261A. Additional penalties are authorized where there are particular harms. For example, if the offense results in serious bodily injury to the victim or involves use of a dangerous weapon, the maximum prison term increases to 10 years. *Id.* §§ 2261(b)(3), 2261A. If permanent disfigurement or life threatening bodily injury results, the maximum prison term authorized is 20 years. *Id.* §§ 2261(b)(2), 2261A. With some exceptions, an additional five years of imprisonment is authorized for violations where the victim is under the age of 18 years. *Id.* §§ 2261A, 2261B. Up to life imprisonment is authorized for fatal violations of the statute. *Id.* §§ 2261(b)(1), 2261A.

[291] Specifically, the statute encompasses use of "the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce." 18 U.S.C. § 2261A(2). The statute does not define "interactive computer service," "electronic communication service," or "electronic communication system," and when listing the elements of a § 2261A(2) offense, federal courts sometimes group the various phrases into a basic requirement that the defendant use a facility of interstate commerce. *E.g.*, United States v. Ackell, 907 F.3d 67, 72–73 (1st Cir. 2018); United States v. Gonzalez, 905 F.3d 165, 180 (3d Cir. 2018). In practice, the statute seemingly reaches harassment and stalking perpetrated using a variety of technological means such as mailings, e-mails, social media, text messages, and the internet. *See, e.g.*, United States v. Conlan, 786 F.3d 380, 384 (5th Cir. 2015) (affirming § 2261A conviction involving an "escalating, year-long campaign of email, text-message, social-media, telephonic, and face-to-face contact with [the victim], her family, work colleagues, and church members"); United States v. Sayer, 748 F.3d 425, 428–29 (1st Cir. 2014) (affirming § 2261A conviction where defendant had used a combination of social media sites, online advertising, and pornography websites to harass the victim); United States v. Moreland, 207 F. Supp. 3d 1222, 1225 (N.D. Okla. 2016) (presenting allegations in § 2261A prosecution where stalking involved "e-mails, social media, and deliveries").

[292] 18 U.S.C. § 2261A(2).

[293] *Id.*; *Id.* § 2266(2).

[294] *Id.* § 2261A(2).

Prosecutors have used § 2261A(2) to charge individuals for a variety of cyberstalking behaviors, such as: a Florida man who stole photographs from "dozens of young women" and used "the photographs to create pornography" that he posted online;[295] a Massachusetts man who conducted "an extensive cyberstalking campaign against his former housemate" and others, in which he posted "fraudulent sexual solicitations in their names, sen[t] unsolicited images of child pornography, and [made] over 120 hoax bomb threats";[296] and a Seattle man who targeted two acquaintances with an online campaign involving "death threats, body shaming, and hate speech."[297]

Swatting: Other specific forms of cyber harassment may also be subject to federal criminal liability. For example, federal prosecutors have used 18 U.S.C. § 875 to charge individuals who engaged in swatting[298]—that is, reporting a false emergency in an attempt to direct an armed police response to a certain target or location, often as a prank or means of harassment.[299] Section 875 imposes a maximum penalty of five years imprisonment for transmitting a threat in interstate commerce to injure someone, or twenty years if that threat involves extortion.[300] In addition, § 2261A may be relevant to swatting, along with other federal statutes such as those proscribing threats involving the mail, interstate transmission of threats involving explosives, and

[295] Press Release, U.S. Dep't of Just., Cyberstalker Sentenced to 10 Years in Prison (Mar. 1, 2016), https://www.justice.gov/opa/pr/cyberstalker-sentenced-10-years-prison; Indictment, United States v. Rubens, No. 4:15-CR-33 (N.D. Fla. Aug. 25, 2015).

[296] Press Release, U.S. Dep't of Just., Massachusetts Man Sentenced to More than 17 Years in Prison for Cyberstalking Former Housemate and Others, Computer Hacking, Sending Child Pornography and Making Over 100 Hoax Bomb Threats (Oct. 3, 2018), https://www.justice.gov/opa/pr/massachusetts-man-sentenced-more-17-years-prison-cyberstalking-former-housemate-and-others; Information, United States v. Lin, No. 18-CR-10092 (D. Mass. Apr. 9, 2018).

[297] Press Release, U.S. Dep't of Just., Seattle Man Pleads Guilty to Cyberstalking Campaign (Sep. 10, 2018), https://www.justice.gov/opa/pr/seattle-man-pleads-guilty-cyberstalking-campaign; Felony Information, United States v. Kurzynski, No. 18-CR-203 (W.D. Wash. Aug. 23, 2018).

[298] *See, e.g.*, Press Release, U.S. Dep't of Just., Massachusetts Man Sentenced to 30 Months for Making Hoax Emergency Services Calls (Oct. 29, 2013), https://www.justice.gov/opa/pr/massachusetts-man-sentenced-30-months-making-hoax-emergency-services-calls; Information, United States v. Hanshaw, Crim. No. 1340018 (D. Mass. Aug. 9, 2013); *see also* Press Release, U.S. Dep't of Just., Georgetown Man Sentenced To 37 Months For Nationwide Swatting Incidents (Nov. 4, 2020), https://www.justice.gov/usao-de/pr/georgetown-man-sentenced-37-months-nationwide-swatting-incidents.

[299] *See* Kimberlin v. Frey, No. GJH-13-3059, 2017 WL 3141909, at *3 n.7 (D. Md. July 21, 2017), *aff'd*, 714 F. App'x 291 (4th Cir. 2018) ("A swatting attack is where a prank call is made to law enforcement in order to dispatch a large number of officers to a targeted individual."); United States v. Neff, No. 3:11-CR-0152-L, 2013 WL 30650, at *3 (N.D. Tex. Jan. 3, 2013), *aff'd*, 544 F. App'x 274 (5th Cir. 2013) ("A 'swatting 911 call' is a false 911 call made to police in which a false report of a violent crime is made to elicit a police Special Weapons and Tactics squad ('SWAT') response to the physical address of a targeted individual, his or her family members, or place of employment."); Press Release, U.S. Dep't of Just., Former Atomwaffen Division Leader Sentenced for Swatting Conspiracy (May 4, 2021), https://www.justice.gov/usao-edva/pr/former-atomwaffen-division-leader-sentenced-swatting-conspiracy ("Swatting is a harassment tactic that involves deceiving emergency dispatchers into believing that a person or persons are in imminent danger of death or bodily harm and causing the dispatchers to send police and emergency services to an unwitting third party's address.").

Swatting may be categorized as a cybercrime since "[s]watters are often sophisticated cybercriminals" who "typically use various social engineering, phishing, Caller I.D. spoofing, and anonymizing methods in order to gain information about their intended targets, deceive the emergency service providers, and cover their tracks." Laura-Kate Bernstein, *Investigating and Prosecuting "Swatting" Crimes*, in 64 J. OF FED. L. & PRAC.: CYBER MISBEHAVIOR 51, 51 (2016).

[300] 18 U.S.C. § 875(b)-(c).

certain hoaxes.[301] Depending on the circumstances, swatting may involve other illegal conduct—such as unauthorized computer access—which may run afoul of other federal laws.[302]

Doxing: Another example of a type of cyber harassment that may incur federal criminal liability in some situations is "doxing,"[303] that is, obtaining another individual's personal identifying information (such as an address, telephone number, or Social Security Number) and posting it online, often for "retribution, harassment or humiliation."[304] For example, prosecutors have used 18 U.S.C. § 119 to prosecute individuals who doxed federal officials such as United States Senators[305] and a federal judge.[306] Section 119 authorizes fines and up to five years of imprisonment for knowingly making publicly available the restricted personal information—such as Social Security Numbers, home addresses, home and mobile phone numbers, or personal emails—of various federal officials and personnel.[307] The statute applies only where the defendant intended to threaten, intimidate, or incite a violent crime against the victim or that victim's immediate family, or where the defendant had intent and knowledge that the restricted personal information would be used in that manner.[308] Doxing may also involve other types of criminal conduct such as computer hacking and stalking, and in such instances federal

[301] *See* Bernstein, *supra* note 299, at 53–54 (surveying charging options for cyberstalking cases).

[302] For example, prosecutors indicted two defendants with charges including conspiracy, aggravated identify theft, and CFAA violations, where they allegedly obtained unauthorized access to Yahoo account information and used it to gain control of Ring doorbell camera devices. Press Release, U.S. Dep't of Just., Grand Jury Indicts 2 in "Swatting" Scheme that Took Over Ring Doorbells Across U.S. to Livestream Police Response to Fake Calls (Dec. 19, 2022), https://www.justice.gov/usao-cdca/pr/grand-jury-indicts-2-swatting-scheme-took-over-ring-doorbells-across-us-livestream. Federal prosecutors claim that the defendants used this access in a swatting scheme in which they "placed false emergency reports or telephone calls to local law enforcement in the areas where the victims lived," "transmitted the audio and video from those devices on social media during the police response," and "verbally taunted responding police officers and victims through the Ring devices during several of the incidents." *Id.*

[303] The term is sometimes spelled "doxxing." *E.g.*, Meira Gebel, *What is doxxing? Here's what you need to know, including how to protect your personal information*, INSIDER.COM (Nov. 13, 2020), https://www.businessinsider.com/what-is-doxxing.

[304] Vangheluwe v. Got News, LLC, 365 F. Supp. 3d 850, 858–59 (E.D. Mich. 2019) (internal quotation marks omitted); *see also* United States v. Cook, 472 F. Supp. 3d 326, 335 (N.D. Miss. 2020) (describing "doxxing" or "doxing" as a "phenomenon" in "which a person's information, such as address or family members' names, is shared publicly").

[305] *E.g.*, Press Release, U.S. Dep't of Just., District Man Sentenced to Four Years for Stealing Senate Information and Illegally Posting Restricted Information of U.S. Senators on Wikipedia (June 19, 2019), https://www.justice.gov/usao-dc/pr/district-man-sentenced-four-years-stealing-senate-information-and-illegally-posting; Criminal Complaint, United States v. Cosko, No. 118R00303, 2018 WL 7959216 (D.D.C. Oct. 3, 2018).

[306] *E.g.*, United States v. Kaetz, No. 2:21-CR-71, 2021 U.S. Dist. LEXIS 65591, at *1, (D.N.J. Apr. 5, 2021); *see also* Matthew Santoni, *NJ Man Gets 16 Months For Posting Judge's Address Online*, LAW360 (Aug. 2, 2021), https://www.law360.com/whitecollar/articles/1409101/nj-man-gets-16-months-for-posting-judge-s-address-online (reporting on sentencing of man convicted for a count of "making restricted personal information publicly available" in connection with posting the name and home address of a federal judge on Facebook).

[307] 18 U.S.C. § 119(a)-(b). The federal officials protected by Section 119 are defined by reference to 18 U.S.C. § 1114. *Id.* For a discussion of the officials and personnel that fit within the protections of § 1114, and therefore § 119, see CRS Report R46829, *Domestic Terrorism: Overview of Federal Criminal Law and Constitutional Issues*, by Peter G. Berris, Michael A. Foster, and Jonathan M. Gaffney, at 23-24.

In 2022, Congress enacted the Daniel Anderl Judicial Security and Privacy Act of 2022 (DAJSPA) as part of the National Defense Authorization Act for 2023. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, 136 Stat. 2395 (2022). DAJSPA does not contain criminal penalties but rather provides various data privacy protections for—and mechanisms for the removal of—certain types of personal or identifying information of federal judges and certain family or household members of federal judges. Daniel Anderl Judicial Security and Privacy Act of 2022, Pub. L. No. 117-263, Title LIX, Subtitle D, 136 Stat. 2395, 2487 (to be codified at 44 U.S.C. §§ 5931–5939).

[308] 18 U.S.C. § 119(a)(1)-(2).

prosecutors have used a variety of statutes to prosecute the conduct,[309] including the CFAA,[310] 18 U.S.C. § 875 (interstate threats),[311] and 18 U.S.C. § 2261A(2) (cyberstalking),[312] discussed above.

Constitutional concerns—particularly related to the First Amendment's protection of freedom of speech—may limit the extent to which some cyber harassment may be subject to criminal enforcement.[313] A review of First Amendment law that could be applicable in this context may be found in other CRS products.[314]

Unlawful Access to Electronic Communications

Cybercriminals sometimes specifically target electronic communications such as emails, instant messages, and texts.[315] The goal of such conduct may vary; schemes to intercept or obtain electronic communications could be aimed at altering foreign policy,[316] snooping,[317] gaining

[309] *See*, *e.g.*, Press Release, U.S. Dep't of Just., New York Man Sentenced To 24 Months in Prison For Internet Offenses, Including "Doxing," "Swatting," Making a False Bomb Threat, and Cyber-Stalking (Jul. 11, 2016), https://www.justice.gov/usao-dc/pr/new-york-man-sentenced-24-months-prison-internet-offenses-including-doxing-swatting (describing guilty plea by individual in connection with doxing scheme of charges including "conspiracy to commit a range of federal offenses, including identity theft; access device fraud; social security number misuse; computer fraud; wire fraud; assaulting federal officials; and interstate transmission of threats").

[310] *E.g.*, Press Release, *supra* note 305.

[311] *E.g.*, Press Release, U.S. Dep't of Just., Keene Man Convicted of Extortion and Threat Offenses (Sep. 28, 2020), https://www.justice.gov/usao-nh/pr/keene-man-convicted-extortion-and-threat-offenses; Verdict, United States v. Cantwell, No. 20-CR-06-01, 2020 WL 7132145 (D.N.H. Sep. 28, 2020).

[312] *See*, *e.g.*, Press Release, U.S. Dep't of Just., Former eBay Employee Pleads Guilty in Aggressive Cyberstalking Campaign (Oct. 27, 2020), https://www.justice.gov/usao-ma/pr/former-ebay-employee-pleads-guilty-aggressive-cyberstalking-campaign (announcing guilty plea of defendant for charges including conspiracy to commit cyberstalking in connection with doxing scheme).

[313] *See*, *e.g.*, United States v. Cook, 472 F. Supp. 3d 326, 335 (N.D. Miss. 2020) (holding that the Free Speech Clause barred the defendant's prosecution under § 2261A(2) for Facebook posts that did not rise to the level of "true threats"—a category of speech that the government can generally prohibit consistent with the First Amendment); United States v. Cassidy, 814 F. Supp. 2d 574, 583–85 (D. Md. 2011) (holding that § 2261A(2) was unconstitutional as applied to the defendant's Twitter posts, which contained protected speech, reasoning that the government does not have a compelling interest in "criminalizing speech that inflicts emotional distress").

[314] *See generally* CRS In Focus IF11072, *The First Amendment: Categories of Speech*, by Victoria L. Killion; CRS Report R45650, *Free Speech and the Regulation of Social Media Content*, by Valerie C. Brannon; CRS Legal Sidebar LSB10723, *Federal Civil Action for Disclosure of Intimate Images: Free Speech Considerations*, by Victoria L. Killion.

[315] *See infra* notes 316–320 and accompanying discussion.

[316] *See*, *e.g.*, Press Release, U.S. Dep't of Just., Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army (Mar. 22, 2016), https://www.justice.gov/opa/pr/computer-hacking-conspiracy-charges-unsealed-against-members-syrian-electronic-army (publicizing charges against three Syrian nationals in connection with a wide ranging cyber scheme involving theft of electronic communications and other conduct aimed at personal profit and altering U.S. policy in a manner favorable to the Syrian government).

[317] *See*, *e.g.*, United States v. Szymuszkiewicz, 622 F.3d 701, 702–03 (7th Cir. 2010), *as amended* (Nov. 29, 2010) (affirming conviction of employee who intercepted his boss's emails to determine whether he would be terminated for having had his driver's license suspended).

commercial advantage,[318] or stealing sensitive information,[319] among other objectives.[320] Illicit access to electronic communications may violate a number of statutes, including the CFAA as discussed above.[321] Other federal criminal laws may also be relevant. For example, the Wiretap Act, at 18 U.S.C. § 2511,[322] imposes criminal penalties for,[323] among other things, the intentional interception of electronic communications by using an electronic device.[324] Federal courts have generally concluded that in order for conduct to qualify as interception in violation of § 2511, it must occur contemporaneously with the transmission of that communication.[325] Section 2511 has been used to prosecute an employee who intercepted his employer's emails in an attempt to determine whether he would be terminated,[326] the Vice President of an online listing service for rare books who allegedly intercepted electronic communications between customers and a rival corporation,[327] and a city councilman who used spyware to access communications "covertly obtained from the computer" of a county administrator.[328]

Modern electronic communications are "equally vulnerable to intrusion when they are at rest as when they are in transmission."[329] Although communications *at rest* generally fall outside the scope of § 2511 (given its focus on proscribing the interception of messages contemporaneously with their transmission), stored communications are protected by other federal statutes.[330]

Additional CRS Products on Unlawful Access to Electronic Communications, and Related Topics:

[318] United States v. Councilman, 418 F.3d 67, 70–71 (1st Cir. 2005) (describing prosecution of Vice President of an e-commerce site, who intercepted electronic communications between customers and a rival company).

[319] *See, e.g.*, Press Release, U.S. Dep't of Just., Ohio Computer Programmer Indicted for Infecting Thousands of Computers with Malicious Software and Gaining Access to Victims' Communications and Personal Information (Jan. 10, 2018), https://www.justice.gov/opa/pr/ohio-computer-programmer-indicted-infecting-thousands-computers-malicious-software-and (describing indictment of Ohio man accused of, among other things, using malware to obtain "potentially embarrassing communications" from victims).

[320] *See, e.g.*, Luis v. Zang, 833 F.3d 619, 623–24 (6th Cir. 2016) (outlining incident where jealous husband "intercept[ed] electronic communications such as emails and instant messages" between his wife and an acquaintance "as leverage to help his attorney secure favorable terms for a divorce").

[321] *See, e.g.*, U.S. Dep't of Just., *supra* note 319.

[322] This statute is part of the Electronic Communications Privacy Act (ECPA), discussed in detail in CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[323] Generally, § 2511 authorizes fines, a maximum prison term of up to five years, or both. 18 U.S.C. § 2511(4)(a).

[324] *Id.* § 2511(1).

[325] *See, e.g.*, Boudreau v. Lussier, 901 F.3d 65, 78 (1st Cir. 2018) (holding that § 2511 "require[s] that communications be intercepted contemporaneously"); *Luis*, 833 F.3d at 628 ("All of the circuit courts that have considered the issue ... have concluded ... that the acquisition of a communication must be contemporaneous with its transmission in order for an 'intercept' to occur."); United States v. Szymuszkiewicz, 622 F.3d 701, 705 (7th Cir. 2010), *as amended* (Nov. 29, 2010) ("Several circuits have said that, to violate § 2511, an interception must be 'contemporaneous' with the communication.").

For a discussion of how courts have construed the "contemporaneous" requirement in the context of different technologies and fact patterns, see Doyle, *supra* note 322, at 9 n.57.

[326] *Szymuszkiewicz*, 622 F.3d at 702–03.

[327] United States v. Councilman, 418 F.3d 67, 70–71 (1st Cir. 2005).

[328] United States v. Trout, 369 F. App'x 493, 493 (4th Cir. 2010) (per curiam).

[329] Doyle, *supra* note 322, at 34.

[330] *E.g.*, 18 U.S.C. § 2701. Section 2701 is part of the Stored Communications Act. Doyle, *supra* note 322, at 1, 34. With exceptions, § 2701 criminalizes conduct such as obtaining electronic communications in storage through intentional, unauthorized access to a facility through which an electronic communication service is provided. 18 U.S.C. § 2701. For more information, see generally Doyle, *supra* note 322, at 34–39.

- CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle;
- CRS Report R45173, *Cross-Border Data Sharing Under the CLOUD Act*, by Stephen P. Mulligan;
- CRS Legal Sidebar LSB10801, *Overview of Governmental Action Under the Stored Communications Act (SCA)*, by Jimmy Balser;
- CRS Legal Sidebar LSB10125, *Law Enforcement Access to Overseas Data Under the CLOUD Act*, by Stephen P. Mulligan.

Other Electronic Fraud

As mentioned above, the CFAA has an anti-fraud provision (§ 1030(a)(4)) encompassing much fraudulent conduct involving unauthorized access to computers.[331] Depending on the circumstances, a number of other federal statutes also criminalize fraudulent conduct in the cyber context.[332] For example, one frequently used prosecutorial tool is the federal wire fraud statute, 18 U.S.C. § 1343, which authorizes criminal penalties[333] for knowing or willing participation in a scheme to defraud using interstate wires.[334] Courts have interpreted "scheme to defraud" to include the "common understanding" of depriving someone of money or property by "dishonest methods" such as trickery and deceit.[335] Use of interstate wires may be demonstrated with evidence of transmission across state lines—for example, through evidence that an individual transmitted information to an out of state computer through the internet.[336] To violate the wire fraud statute, it need only be reasonably foreseeable that the interstate wires would be used in furtherance of the scheme to defraud, which generally requires only that the wires be "'incident[al]' to an essential part of the scheme .... "[337] In the cyber context, the wire fraud statute has been used to prosecute two Massachusetts men who purportedly used computers, the internet,

[331] *See supra* Section "Computer Fraud, 18 U.S.C. § 1030(a)(4)."

[332] Although a complete review exceeds the scope of this report, other possible federal criminal laws applicable to fraud in the cyber context might include bank fraud (18 U.S.C. § 1344), electronic message fraud (*Id.* § 1037), and access device fraud (*Id.* § 1029). In the cyber context, federal prosecutors have also used statutes such as 18 U.S.C. § 1028A, prohibiting aggravated identity theft. *See*, *e.g.*, Press Release, U.S. Dep't of Just., New York Man Sentenced to 36 Months for Stealing Nude Photos of Dozens of Victims (Aug. 19, 2021), https://www.justice.gov/opa/pr/new-york-man-sentenced-36-months-stealing-nude-photos-dozens-victims (announcing sentencing of New York man for "computer fraud and aggravated identity theft in connection with his hacking of online social media accounts and theft of nude images of dozens of women"). The Supreme Court is currently considering a case examining the appropriate scope of the aggravated identity theft statute. See Dubin v. United States, No. 22-10 (U.S. argued Feb. 27, 2023).

[333] Violations of the wire fraud statute are punishable by fines, imprisonment, or both. 18 U.S.C. § 1343. Ordinarily, the maximum prison term authorized under § 1343 is 20 years; however, imprisonment for up to 30 years is authorized for violations relating to a presidentially declared Stafford Act major disaster or emergency, or a "benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection" with such a disaster or emergency. *Id.*

[334] *Id.* § 1343.

[335] Carpenter v. United States, 484 U.S. 19, 27 (1987) (internal quotation marks omitted).

[336] *See*, *e.g.*, United States v. Valdes-Ayala, 900 F.3d 20, 33–34 (1st Cir. 2018) (concluding that evidence supported defendant's use of interstate wires where scheme involved emails transmitted between computers and servers in Puerto Rico and several states); *see also* United States v. Hussain, 972 F.3d 1138, 1145 (9th Cir. 2020) (affirming conviction of defendant for wire fraud in connection with scheme where "[s]ix counts stemmed from phone or video conference calls among participants in the United Kingdom and California, five counts focused on emails originating or terminating in California, and three involved press releases distributed from England to California"); *see also* United States v. Riggs, 743 F. Supp. 556, 562 (N.D. Ill. 1990) (rejecting motion to dismiss wire fraud indictment where defendant's use of interstate wires was alleged to involve e-mail).

[337] United States v. Carpenter, 190 F. Supp. 3d 260, 265 (D. Conn. 2016) (quoting Schmuck v. United States, 489 U.S. 705, 712 (1989)), *aff'd sub nom.* United States v. Bursey, 801 F. App'x 1 (2d Cir. 2020); *accord* United States v. Jinian, 725 F.3d 954, 960 (9th Cir. 2013) ("A wire communication is 'in furtherance' of a fraudulent scheme if it is 'incident to the execution of the scheme.'" (*quoting* United States v. Lo, 231 F.3d 471, 478 (9th Cir.2000))).

and phones to steal social media accounts and at least $550,000 in cryptocurrency,[338] two Romanian residents who netted millions of dollars in part through the use of fake online auction listings infected with malware,[339] four members of the Chinese People's Liberation Army alleged to have stolen personal data and trade secrets through the Equifax hack,[340] and many others.[341]

Additional CRS Products on Fraud:

- CRS Report R41930, *Mail and Wire Fraud: A Brief Overview of Federal Criminal Law*, by Charles Doyle;
- CRS Report R45479, *Bribery, Kickbacks, and Self-Dealing: An Overview of Honest Services Fraud and Issues for Congress*, by Michael A. Foster;
- CRS Legal Sidebar LSB10446, *An Overview of Federal Criminal Laws Implicated by the COVID-19 Pandemic*, by Peter G. Berris.

[338] Press Release, U.S. Dep't of Just., Two Massachusetts Men Arrested and Charged with Nationwide Scheme to Steal Social Media Accounts and Cryptocurrency (Nov. 14, 2019), https://www.justice.gov/opa/pr/two-massachusetts-men-arrested-and-charged-nationwide-scheme-steal-social-media-accounts-and.

[339] Press Release, U.S. Dep't of Just., Two Romanian Cybercriminals Convicted of All 21 Counts Relating to Infecting Over 400,000 Victim Computers with Malware and Stealing Millions of Dollars (Apr. 11, 2019), https://www.justice.gov/opa/pr/two-romanian-cybercriminals-convicted-all-21-counts-relating-infecting-over-400000-victim.

[340] Press Release, U.S. Dep't of Just., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

[341] *See* Press Release, U.S. Dep't of Just., International Hacker Pleads Guilty for Massive Hacks of U.S. Retail Networks (Sep. 11, 2009), https://www.justice.gov/opa/pr/international-hacker-pleads-guilty-massive-hacks-us-retail-networks (announcing guilty plea of Miami resident for wire fraud and other charges connected to his hack of U.S. retailers); Press Release, U.S. Dep't of Just., Three Individuals Charged for Alleged Roles in Twitter Hack (Jul. 31, 2020), https://www.justice.gov/opa/pr/three-individuals-charged-alleged-roles-twitter-hack (summarizing wire fraud conspiracy charges against three individuals in connection with a hack of Twitter); Press Release, U.S. Dep't of Just., International 'Malvertiser' Extradited from Netherlands to Face Hacking Charges in New Jersey (May 3, 2019), https://www.justice.gov/usao-nj/pr/international-malvertiser-extradited-netherlands-face-hacking-charges-new-jersey (detailing extradition of Ukrainian national to face wire fraud and wire fraud conspiracy charges (among others) connected to his use of "malvertising," or online advertisements infected with malware); Press Release, U.S. Dep't of Just., Resident of India Pleads Guilty in International Online Brokerage "Hack, Pump and Dump" Scheme (Feb. 5, 2010), https://www.justice.gov/opa/pr/resident-india-pleads-guilty-international-online-brokerage-hack-pump-and-dump-scheme (noting guilty plea by Indian resident to wire fraud conspiracy count connected to "an international fraud scheme to 'hack' into online brokerage accounts in the United States and use those accounts to manipulate stock prices"); Press Release, U.S. Dep't of Just., Sixth and Final Defendant Sentenced to Prison for Sophisticated International Cellphone Fraud Scheme (Jan. 24, 2020), https://www.justice.gov/opa/pr/sixth-and-final-defendant-sentenced-prison-sophisticated-international-cellphone-fraud-scheme (describing sentencing of a citizen and resident of the Dominican Republic on charges including wire fraud and wire fraud conspiracy related to "sophisticated global cellphone fraud scheme that involved compromising cellphone customers' accounts in the United States and 'cloning' their phones to make fraudulent international calls"); Press Release, U.S. Dep't of Just., Four Members of International Computer Hacking Ring Indicted for Stealing Gaming Technology, Apache Helicopter Training Software (Sep. 30, 2014), https://www.justice.gov/opa/pr/four-members-international-computer-hacking-ring-indicted-stealing-gaming-technology-apache (publicizing indictment of "[f]our members of an international computer hacking ring" for charges including wire fraud stemming from a scheme to break "into computer networks of prominent technology companies and the U.S. Army and steal[] more than $100 million in intellectual property and other proprietary data"); Press Release, U.S. Dep't of Just., Nigerian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy (Dec. 9, 2019), https://www.justice.gov/opa/pr/nigerian-citizen-extradited-connection-prosecution-africa-based-cybercrime-and-business-email (announcing extradition of Nigerian citizen to "stand trial for an indictment charging him with wire fraud" and other charges related to a business-email compromise scheme causing hundreds of thousands of dollars in losses).

Challenges in Prosecuting Cybercrimes Originating Abroad

As a general matter, "[f]ederal laws are presumed to apply only within the United States, unless Congress clearly provides otherwise"—a principle sometimes described as a presumption against extraterritoriality.[342] Crimes that occur in the United States are not extraterritorial even if committed by foreign actors.[343] For example, in *United States v. Ivanov*, a federal district court concluded that the CFAA could apply to a defendant who was "physically present in Russia and using a computer there" where the "intended and actual detrimental effects of [his] substantive offenses ... occurred within the United States."[344] In particular, the court emphasized that the computers the defendant allegedly gained unauthorized access to were physically located in Connecticut.[345] In practice, DOJ has used many of the statutes described above, including the CFAA, to prosecute international defendants whose conduct—or the detrimental effects of that conduct—occurred at least in part in the United States.[346]

Even if a crime does occur *entirely* overseas, there are a number of federal statutes that expressly authorize extraterritorial application.[347] Although there is minimal case law examining the

[342] CRS Report 94-166, *Extraterritorial Application of American Criminal Law*, by Charles Doyle, at summary; *see also* RJR Nabisco, Inc. v. Eur. Cmty., 136 S. Ct. 2090, 2100 (2016) ("This principle finds expression in a canon of statutory construction known as the presumption against extraterritoriality: Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application.").

[343] *RJR Nabisco*,136 S. Ct. at 2101 ("If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory."); *see also*, *e.g.*, United States v. Hussain, 972 F.3d 1138, 1140, 1145 (9th Cir. 2020) (affirming conviction of U.K. citizen and concluding that application of wire fraud statute was not improperly extraterritorial given that defendant's "use of the wires in furtherance of his fraud had a sufficient domestic nexus").

The question of where a crime occurs for extraterritorial analysis may be complex, particularly where crime crosses borders. For a discussion of these issues, see generally Julie Rose O'Sullivan, *The Extraterritorial Application of Federal Criminal Statutes: Analytical Roadmap, Normative Conclusions, and A Plea to Congress for Direction*, 106 GEO. L.J. 1021, 1025 (2018).

[344] United States v. Ivanov, 175 F. Supp. 2d 367, 370, 373 (D. Conn. 2001).

[345] *Id.* at 371.

[346] *See*, *e.g.*, Press Release, U.S. Dep't of Just., Ghanaian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy (Aug. 26, 2020), https://www.justice.gov/opa/pr/ghanaian-citizen-extradited-connection-prosecution-africa-based-cybercrime-and-business-email (discussing extradition of Ghanaian citizen for trial in connection with "an indictment charging him with wire fraud, money laundering, computer fraud and aggravated identity theft"); Press Release, U.S. Dep't of Just., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking (providing update on prosecution of Chinese national for wire fraud, EEA, and CFAA violations); Press Release, U.S. Dep't of Just., U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Oct. 4, 2018), https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and (giving overview of prosecution of Russian intelligence officers for wire fraud, CFAA violations, and aggravated identity theft, among other charges); Press Release, U.S. Dep't of Just., Romanian National "Guccifer" Extradited to Face Hacking Charges (Apr. 1, 2016), https://www.justice.gov/opa/pr/romanian-national-guccifer-extradited-face-hacking-charges (announcing extradition of Romanian man to face indictment alleging, among other things, cyberstalking, wire fraud, and CFAA violations).

[347] Doyle, *supra* note 342, at 45–71 (collecting statutes).

extraterritoriality of the CFAA,[348] the federal district court in *Ivanov* concluded that there was "clear evidence that the statute was intended by Congress to apply extraterritorially."[349] Among other things,[350] the court considered several 1996 amendments to the CFAA, including one that expanded the definition of "protected computer" to include computers used in interstate or foreign commerce or communication.[351] The court concluded that in this context, the word "foreign" means "international" and therefore the CFAA provisions using the term "protected computer" or otherwise referencing "foreign commerce"[352] are extraterritorial in scope.[353] One unresolved issue is whether §§ 1030(a)(1) (cyber espionage) and 1030(a)(3) (government computer trespass)—which do not mention protected computers or foreign commerce—may apply extraterritorially. Given the rare use of these provisions in general—and the potential availability of other charges[354]—there may be little practical need for federal prosecutors to test their extraterritorial reach.

The success of prosecutions of cybercrimes originating abroad may turn less on the legal scope of the relevant statutes, and more on practical considerations and matters of foreign relations. As another CRS product explains in detail, investigating and prosecuting criminal conduct in other countries raises questions of national sovereignty and may involve "legal, practical, and often diplomatic obstacles that can be daunting."[355] For example, the United States lacks extradition treaties with some countries, which may make domestic prosecution of criminals residing in those countries challenging.[356] This difficulty is not to say that prosecution can never happen. For instance, Russian national Peter Levashov was accused of operating botnets[357] "which enabled him to harvest personal information from infected computers, disseminate spam, and distribute

[348] As of March 14, 2023, a search of the Westlaw legal database for cases citing § 1030 and using the phrase "extraterritorial" in the same paragraph as a citation to that statute yielded seven results. For a discussion of the extraterritoriality of CFAA's civil provision, see, e.g., Ryanair DAC v. Expedia Inc., No. C17-1789RSL, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018); Ryanair DAC v. Booking Holdings Inc., No. CV 20-1191-LPS, 2021 WL 7209367, at *7 (D. Del. Dec. 27, 2021).

[349] *Ivanov*, 175 F. Supp. 2d at 373.

[350] The court also looked to legislative history, including a 1996 Senate Judiciary Committee report expressing concern that the preexisting version of the CFAA omitted "computers used in foreign communications or commerce, despite the fact that hackers are often foreign-based." *Id.* at 374 (*quoting* S. REP. 104-357, 4).

[351] *Id.* (citing Economic Espionage Act of 1996, Pub. L. No. 104–294, 110 Stat. 3491, 3508 (amending 18 U.S.C. §§ 1831–1839)); *see also* United States v. Gasperini, 729 F. App'x 112, 114 (2d Cir. 2018) (mem.) (noting that although it need not decide the question, based on the definition of "protected computer" there "is a strong argument that § 1030(a)(2) applies extraterritorially"); *In re* Apple Inc. Device Performance Litig., 347 F. Supp. 3d 434, 448 (N.D. Cal. 2018), *on reconsideration in part*, 386 F. Supp. 3d 1155 (N.D. Cal. 2019) (determining that CFAA civil provisions applies extraterritorially based on definition of "protected computer" in civil suit brought pursuant to § 1030(A)(5)(A), (C)).

[352] *E.g.*, 18 U.S.C. § 1030(a)(6).

[353] *Ivanov*, 175 F. Supp. 2d at 374.

[354] *See supra* Sections "Cyber Espionage, 18 U.S.C § 1030(a)(1)"; "Government Computer Trespassing, 18 U.S.C. § 1030(a)(3)."

[355] Doyle, *supra* note 342, at 24.

[356] *Id.* at 32. For a detailed overview of extradition law, see generally CRS Report 98-958, *Extradition To and From the United States: Overview of the Law and Contemporary Treaties*, by Michael John Garcia and Charles Doyle.

[357] Botnets are "network[s] of compromised computers, 'often programmed to complete a set of repetitive tasks' without 'the owner's knowledge or permission.'" Beale & Berris, *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.3d 482, 485 (2d Cir. 2018) (describing botnets as "network[s] of infected computers under the attacker's control").

malware used to facilitate multiple scams."[358] Although Russia lacks an extradition treaty with the United States,[359] Levashov was extradited from Spain where he was arrested with "cooperation of Spanish authorities ... while [he was] on holiday."[360] In 2018, Levashov pleaded guilty in federal court to several charges, including under the CFAA, and the wire fraud and aggravated identity theft statutes.[361] Where prosecution of an international defendant is impractical, DOJ may still be able to target property illicitly obtained from cybercrimes through civil asset forfeiture—a statutory regime enabling DOJ to file lawsuits against certain property that is derived from, or used in, various crimes.[362] For example, DOJ used this authority in June 2021 to obtain a warrant to seize Bitcoin that Colonial Pipeline paid to ransomware attackers.[363]

Additional CRS Products on Application of Federal Criminal Laws to Conduct Occurring Abroad:

- CRS Report 94-166, *Extraterritorial Application of American Criminal Law*, by Charles Doyle;
- CRS Report 98-958, *Extradition To and From the United States: Overview of the Law and Contemporary Treaties*, by Michael John Garcia and Charles Doyle;
- CRS Legal Sidebar LSB10308, *Extradition of U.S. Citizens*, by Charles Doyle;
- CRS Legal Sidebar LSB10417, *Red Army Equifax Hackers Indicted*, by Charles Doyle;
- CRS Legal Sidebar LSB10869, *If You Do the Space Crime, You May Do the Space Time*, coordinated by Peter G. Berris.

Congressional Considerations

Botnet Trafficking

One "tool" used by some cybercriminals is a botnet—a "network of compromised computers, 'often programmed to complete a set of repetitive tasks' without 'the owner's knowledge or permission.'"[364] Botnets pose a significant risk because they are sometimes used for attacks on the internet itself—for example, in DDoS attacks against core internet infrastructure.[365] The creation of a botnet and the use of a botnet to commit crimes generally violate the CFAA or other

[358] Press Release, U.S. Dep't of Just., Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses (Sep. 12, 2018), https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime.

[359] Garcia & Doyle, *supra* note 356, at app'x B.

[360] Beale & Berris, *supra* note 1 at 161, 189.

[361] Press Release, *supra* note 358. A federal district court judge sentenced Levashov to time served and an additional term of supervised-release. Rachel Scharf, *Admitted Russian Botnet Mastermind Ducks Prison Time*, LAW360 (July 20, 2021), https://www.law360.com/articles/1404676/admitted-russian-botnet-mastermind-ducks-prison-time.

[362] *See generally* CRS Report 97-139, *Crime and Forfeiture*, by Charles Doyle.

[363] Berris & Gaffney, *supra* note 253, at 6–7; *see also* Press Release, U.S. Dep't of Just., Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (announcing recovery of cryptocurrency paid as ransom in Colonial Pipeline incident and attaching warrants and affidavits listing legal authority to seize that cryptocurrency).

[364] Beale & Berris, *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.3d 482, 485 (2d Cir. 2018) (describing botnets as "network[s] of infected computers under the attacker's control.").

[365] *See* Beale & Berris, *supra* note 1, at 190 ("In contrast, botnets present the reverse issue: devices connected to the internet may be used to disrupt the internet itself.").

federal statutes.[366] However, at times, individuals develop botnets that are rented or sold[367] to other individuals who, in turn, then use them for various crimes such as DDoS attacks and identity theft.[368] Federal courts have not resolved whether the CFAA criminalizes such botnet trafficking, and the issue is particularly uncertain in the case of botnets offered for rent or sale by individuals who did *not* also create them (the CFAA generally criminalizes the creation of a botnet).[369] For example, in a 2015 blog post, DOJ recounted one undercover investigation that revealed a seller offering a botnet comprised of thousands of computers; prosecutors were unable to bring charges against the seller because it was unclear whether he had created the botnet or was simply selling it.[370]

Thus, DOJ has seemingly acknowledged that some botnet trafficking conduct may fall outside the scope of the CFAA.[371] A review of the language of the CFAA reveals the reason. The only CFAA provision that expressly prohibits trafficking—§ 1030(a)(6)—covers only passwords and related information, not botnets.[372] Another relevant CFAA subsection—§ 1030(a)(5)'s prohibition against damaging certain computers—requires that the defendant acts with intent to damage.[373] However, those trafficking in botnets might lack such intent, if they simply intend to profit or are unaware of how the botnet will be used.[374] Nevertheless, DOJ has reached several plea agreements with defendants accused of botnet trafficking.[375] The counts included in those plea agreements have generally been some combination of conspiracy (under 18 U.S.C. § 371) to violate the CFAA or the wire fraud statute,[376] attempt to damage computers by transmission of

[366] *Prosecuting the Sale of Botnets and Malicious Software*, U.S. DEP'T OF JUST. (Mar. 18, 2015), https://www.justice.gov/archives/opa/blog/prosecuting-sale-botnets-and-malicious-software. For instance, in one case involving the operation of a botnet for various illicit schemes, DOJ prosecuted a defendant under the CFAA as well as federal statutes criminalizing wire fraud, conspiracy, and identity theft. Press Release, U.S. Dep't of Just., Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses (Sep. 12, 2018), https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime.

[367] *See* Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 479, 503 (2019) ("There are cases where brokers who sell access to botnets are not the criminals who created them.").

[368] U.S. Dep't of Just., *supra* note footnote 366.

[369] *See id.* ("Current criminal law prohibits the creation of a botnet because it prohibits hacking into computers without authorization. It also prohibits the use of botnets to commit other crimes. But it is not similarly clear that the law prohibits the sale or renting of a botnet.").

[370] *Id.*

[371] *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 computers."); *see also* Press Release, U.S. Dep't of Just., Assistant Attorney General Leslie R. Caldwell Testifies Before the Senate Committee on the Judiciary Subcommittee on Crime and Terrorism (July 15, 2014), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-testifies-senate-committee-judiciary ("The CFAA does not clearly cover such trafficking in access to botnets, even though trafficking in infected computers is clearly illegitimate, and can be essential to furthering other criminal activity.").

[372] 18 U.S.C. § 1030(a)(6).

[373] *Id.* § 1030(a)(5).

[374] *See* Matwyshyn & Pell *supra* note 367, at 503 ("There are several uses for botnets, many of which may not involve financial fraud, and the traffickers may have no knowledge of the intent of use by their customers."); Press Release, *supra* note 371 (explaining that traffickers "may not know or care why their customers are seeking unauthorized access to other people's computers").

[375] *See*, *e.g.*, Press Release, U.S. Dep't of Just., 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.

[376] *Id.*; Press Release, U.S. Dep't of Just., Russian Citizen Sentenced to 46 Months in Prison for Involvement in Global (continued...)

programs, codes or commands in violation of the CFAA,[377] and "advertising a device used to intercept electronic communications" in violation of 18 U.S.C. § 2512.[378]

Although the conspiracy statute invoked by DOJ in some such plea agreements might appear as though it could have widespread applicability in the context of botnet trafficking, a defendant is not guilty of conspiracy unless: (1) he has agreed to commit a specific offense with at least one other person; (2) he knowingly participated in the conspiracy while intending to commit that offense; and (3) a conspirator commits an overt act in furtherance of the conspiracy.[379] The second element—intent—may present an obstacle in some cases because, as discussed, botnet traffickers may be unaware of how the buyer or renter plans to use the botnet and may be intending only to profit.[380] Thus, the seller may lack the requisite intent to commit an underlying offense.[381] Botnet trafficking by itself, for the reasons outlined above, does not appear to violate the CFAA and therefore would likely not amount to an underlying federal offense. Even in instances where the conspiracy statute does reach botnet trafficking—for example, if a botnet trafficker rents botnet access with the intent that it should be used to damage a computer in violation of § 1030(a)(5)—the statute authorizes a maximum prison term of five years,[382] less than under some subsections of the CFAA.[383]

At least one state has enacted a law aimed at botnet trafficking,[384] and the issue has generated legislative proposals in previous administrations[385] and Congress.[386] For example, one proposal introduced in the 117th Congress, titled the International Cybercrime Prevention Act, contained a provision that would have amended the CFAA to prohibit "intentionally traffic[king] in the means of access to a protected computer."[387] Although the proposal did not define "means of access," the intent appears to have been to include botnets.[388] The prohibition would have been subject to two main limitations.[389] First, the trafficker would have had to "know or [have had] reason to know the protected computer [was] damaged in a manner prohibited by" the CFAA.[390] Second, the trafficker would have had to know or have had reason to know that the purchaser or renter

Botnet Conspiracy (Aug. 3, 2017), https://www.justice.gov/opa/pr/russian-citizen-sentenced-46-months-prison-involvement-global-botnet-conspiracy.

[377] *See* Press Release, U.S. Dep't of Just., Arizona Man Sentenced to 30 Months in Prison for Selling Access to Botnets (Sept. 6, 2012), https://www.justice.gov/opa/pr/arizona-man-sentenced-30-months-prison-selling-access-botnets.

[378] *See* Press Release, *supra* note 375.

[379] 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.

[380] *See supra* note 374 and accompanying discussion.

[381] *Id.*

[382] 18 U.S.C. § 371.

[383] *See supra* Section "Remedies and Penalties."

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

[385] President Barack Obama, Remarks by the President at the National Cybersecurity Communications Integration Center (Jan. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent ("[W]e're 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 and spyware.").

[386] *See, e.g.*, International Cybercrime Prevention Act, S. 2139, 117th Cong. (2021).

[387] *Id.* § 6.

[388] The relevant provision is titled "Stopping Trafficking in Botnets; Forfeiture." *Id.*

[389] *Id.*

[390] *Id.*

intended to use the means of access to violate certain laws or to "damage a protected computer" in violation of the CFAA.[391]

The International Cybercrime Prevention Act also contained a provision that appeared intended to "[e]nhance prosecutors' ability to shut down botnets."[392] This provision—§ 4 of the bill—would have amended Section 1345 of Title 18 of the U.S. Code, a statute that permits federal prosecutors to bring civil actions to enjoin certain types of fraud.[393] Under the statute, a district court may enter pre-trial "restraining order[s] or prohibition[s], or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought."[394] For instance, DOJ used § 1345 to obtain a temporary injunction to interrupt the operation of the Kelihos botnet,[395] "a global network of tens of thousands of infected computers under the control of a cybercriminal that was used to facilitate malicious activities including harvesting login credentials, distributing hundreds of millions of spam e-mails, and installing ransomware and other malicious software."[396] The court ordered various forms of relief such as operating substitute servers to "replace the Defendant's command and control infrastructure for the Kelihos botnet and sever the Defendant's connection to the infected computers in the Kelihos botnet."[397] If enacted, § 4 of the International Cybercrime Prevention Act would have permitted DOJ to seek § 1345 relief for actual or imminent violations of § 1030(a)(5) assuming the conduct damaged (or *would* damage) at least 100 protected computers in a one-year period.[398] Section 4 described one type of qualifying damage as "installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers," a description that seemingly encompasses botnets.[399] The other type of damage included in § 4 was "impairing the availability or integrity of the protected computers without authorization," which could potentially describe the impact on a protected computer by co-opting it to serve as part of a botnet.[400] Another bill introduced in the 117th Congress, the CCP Trade Secrets Act, contained largely similar provisions.[401] These proposals tracked legislation previously introduced in earlier Congresses.[402]

---

[391] *Id.*

[392] Press Release, Senator Sheldon Whitehouse, Whitehouse, Graham, Blumenthal, Tillis Reintroduce Legislation To Fight Cybercrime (June 17, 2021), https://www.whitehouse.senate.gov/news/release/whitehouse-graham-blumenthal-tillis-reintroduce-legislation-to-fight-cybercrime-.

[393] *See* United States v. Payment Processing Ctr., LLC, 435 F. Supp. 2d 462, 464 (E.D. Pa. 2006) (indicating that "Section 1345 is a powerful weapon in the government's anti-fraud arsenal" that authorizes "injunctive relief to enjoin specified ongoing or contemplated crimes"); *see also* United States v. Palumbo, 448 F. Supp. 3d 257, 260 (E.D.N.Y. 2020) ("Under 18 U.S.C. § 1345, a court may issue a preliminary injunction against ongoing violations of the wire fraud statute.").

[394] 18 U.S.C. § 1345(b); *Payment Processing Ctr., LLC*, 435 F. Supp. at 464.

[395] United States v. Levashov, No. 3:17-CV-00074-TMB, 2017 WL 1398662, at *2 (D. Alaska Apr. 12, 2017).

[396] *See* Press Release, U.S. Dep't of Just., Justice Department Announces Actions to Dismantle Kelihos Botnet (Apr. 10, 2017), https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

[397] *Levashov*, 2017 WL 1398662, at *2.

[398] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 4 (2021).

[399] *Id.*

[400] *Id.*

[401] CCP Trade Secrets Act, S. 1245, 117th Cong. (2021).

[402] *E.g.*, Defending American Security from Kremlin Aggression Act of 2019, S. 482, 116th Cong. (2019); the Botnet Prevention Act of 2016, S. 2931, 114th Cong. (2016).

"Hacking Back"

Another issue that has garnered legal,[403] academic,[404] media,[405] and legislative[406] attention is that of "hacking back"—where the victim of hacking launches an invasive counterattack against the initial hacker.[407] Hacking back has been the subject of significant debate.[408] Critics argue that hacking back could result in escalation and retaliation[409] and harm innocent parties through misattribution of the source of a cyber-attack.[410] Others have cautioned that hacking back could cause private actors to inadvertently wade into the realm of cyberwarfare and foreign relations if they hack back against an initial aggressor who turns out to be the agent of a foreign state.[411] Much of the scholarship on hacking back has been in this vein,[412] but hacking back has its proponents who argue, among other things, that hacking back is necessary to "establish attribution of an attack, ... retrieve and destroy stolen files, [and] monitor the behavior of an attacker."[413] In addition, it has been suggested that hacking back could be particularly useful in its "ability to prevent future [cyber] attacks by combatting existing botnets."[414]

---

[403] *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).

[404] *See, e.g.*, Beale & Berris, *supra* note 1, at 189-99.

[405] *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.

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

[407] *See* Beale & Berris, *supra* note 1, at 189 n.190 (describing hacking back). Related terms include "counterstrikes, 'active defense,' 'back hacking,' 'retaliatory hacking,' or 'offensive countermeasures.'" *Id.* at 190 (quoting Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?* 20 RICH. J.L. & TECH. 12, 13 (2014)).

[408] *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 hacking back "[t]he worst idea in cybersecurity") *and* Martin Giles, *Five Reasons "Hacking Back" is a Recipe for Cybersecurity Chaos*, MIT TECH. REV. (June 21, 2019), https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/ (describing hacking back as a "terrible idea"), *with* KERR, *supra* note 12, at 140 (summarizing debate over hacking back and collecting articles arguing in favor of hacking back) *and* Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 277 (2000) ("In other words, just as settlers in the American 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 protect themselves.").

[409] 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 security advocates that hacking back "will merely serve 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 for hacking back").

[410] *See, e.g.*, Beale & Berris, *supra* note 1, at 198 (summarizing view that due to difficulty in accurately attributing the source of a cyber-attack, "remedial actions risk collateral damage to innocent parties").

[411] *See* PATRICK LIN, ETHICS OF HACKING BACK: SIX ARGUMENTS FROM ARMED CONFLICT TO ZOMBIES 15 (2016), http://ethics.calpoly.edu/hackingback.pdf ("Regardless of attribution, hacking back against a foreign target may be misinterpreted by the receiving nation as a military response from our state, to serious political and economic backlash.").

[412] *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), https://perma.cc/SAX8-4LW3 ("First, 'hacking back' by the private sector to intentionally cause substantial harm and destroy other parties' data is clearly unauthorized and rightly prohibited."); *accord* Giles, *supra* note 408 (critiquing hacking back).

[413] Press Release, Congressman Josh Gottheimer, Graves, Gottheimer Introduce the Active Cyber Defense Certainty Act (June 13, 2019), https://gottheimer.house.gov/posts/graves-gottheimer-introduce-the-active-cyber-defense-certainty-act.

[414] Beale & Berris, *supra* note 1, at 191.

The debate over hacking back is largely academic, as it appears that much hacking back is currently illegal—at least when conducted by private actors.[415] Although federal courts have not resolved the issue, the weight of persuasive authority suggests that the same provisions of the CFAA that prohibit hacking—such as § 1030(a)(5)'s prohibition against certain damage to computers—also generally prohibit hacking back by the victim of the initial attack.[416] One legislative proposal introduced in the 117th Congress would have required the Department of Homeland Security to study and report to Congress on the "potential benefits and risks of amending" the CFAA "to allow private entities to take proportional actions in response to an unlawful network breach, subject to oversight and regulation by a designated Federal agency."[417] Some past legislative proposals would have authorized certain self-help measures. In the 116th Congress, the Active Cyber Defense Certainty Act would have created two new exceptions to the CFAA clarifying that the law does not prohibit hacking back.[418] First, the Active Cyber Defense Certainty Act would have amended the CFAA to expressly permit certain attributional technologies used to identify cyber intruders.[419] Second, with exceptions, the proposal would have created an exclusion from CFAA prosecution for active cyber defense measures, which include defensive measures "consisting of accessing without authorization" the attacker's computer to gather information necessary to determine attribution, disrupt certain continued authorized activity, or monitor the behavior of an attacker to create "cyber defense techniques."[420]

---

[415] *See, e.g.*, U.S. DEP'T OF JUST., BEST PRACTICES FOR VICTIM RESPONSE, *supra* note 403, at 23 (cautioning that "[r]egardless of the victim's motive," it is possible that "accessing, modifying, or damaging a computer it does not own or operate" will "violate federal law and possibly also the laws of many states and foreign countries, if the accessed computer is located abroad").

The CFAA has a carve-out for certain law enforcement activity, which provides: "This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States." 18 U.S.C. § 1030(f).

Although beyond the scope of this report, 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 protected computer authorizes the interception of the computer trespasser's 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 trespasser's communications will be relevant to the investigation; and
>
> (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C. § 2511(2)(i).

[416] *E.g.*, U.S. DEP'T OF JUST., BEST PRACTICES FOR VICTIM RESPONSE, *supra* note 403, 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 & Berris, *supra* note 1, at 191; CTR. FOR CYBER & HOMELAND SEC., GEO. WASH. UNIV., *supra* note 412; *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).

[417] Study on Cyber-Attack Response Options Act, S. 2292, 117th Cong. (2021).

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

[419] *Id.* § 3.

[420] *Id.* § 4.

Such cyber defense measures would have generally required notification to, and pre-approval by, the FBI.[421]

Critical Infrastructure

The ransomware attack on Colonial Pipeline underscored the potential vulnerability of critical infrastructure to cybercrime.[422] Critical infrastructure "refers to the machinery, facilities, and information that enable vital functions of governance, public health, and the economy."[423] To the extent that computers comprise critical infrastructure, those computers are likely protected by the CFAA.[424] As a result, intentionally damaging computers that are a part of critical infrastructure will likely be a federal crime under the CFAA.[425]

However, a number of bills in the 117th Congress would have amended the CFAA to impose additional penalties where violations target or harm other critical infrastructure.[426] For example, among other things, the Protecting Critical Infrastructure Act of 2021 would have imposed fines and a mandatory minimum prison sentence of thirty years for CFAA violations involving "critical infrastructure."[427] The bill defined "critical infrastructure" by reference to another statute as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[428] It appears that the thirty-year mandatory minimum in the bill would have applied to any CFAA violation involving critical infrastructure.[429] Given the broad array of conduct criminalized by the CFAA, the mandatory minimum might have raised questions about what relationship would be required between the conduct, computer, and critical infrastructure in order for the offense to *involve* critical infrastructure. What if the conduct targeted a computer that was part of a critical infrastructure system, but there was no effect on the critical infrastructure; for example, where the computer did not serve a vital operational function or the conduct did not involve damage to a computer? To the extent that the legislation encompassed minimal connections, the mandatory minimum could potentially have applied not only to incidents that impacted the critical infrastructure itself but also those that were more tangentially related (for example, unauthorized access of information from a computer owned by a company with critical infrastructure operations). Such a reading would mark a significant departure from the current CFAA penalty

[421] *Id.* § 5.

[422] *See Critical Infrastructure Security and Resilience*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/infrastructure-security# (last visited, Dec. 28, 2022).

[423] CRS Report R45809, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys.

[424] *See supra* Section "Key CFAA Terms" (discussing breadth of computers protected by CFAA).

[425] *Id.*; *see also* United States v. Gottesfeld, 18 F.4th 1, 4 (1st Cir. 2021), *cert. denied*, 143 S. Ct. 85 (2022) (affirming § 1030(a)(5) conviction of defendant for a DDoS attack he committed against Boston Children's Hospital and Wayside Youth and Family Support Network); United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) (affirming CFAA conviction of defendant who gained unauthorized access into Madison, Wisconsin's "computer-based radio system for police, fire, ambulance, and other emergency communications").

[426] *E.g.*, International Cybercrime Prevention Act, S. 2139, 117th Cong. (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. (2021).

[427] Protecting Critical Infrastructure Act of 2021, H.R. 1042, 117th Cong. § 2 (2021).

[428] *Id.*; 42 U.S.C. § 5195c.

[429] Protecting Critical Infrastructure Act of 2021, H.R. 3388, 117th Cong. § 2 (2021).

structure, which generally imposes stiffer penalties for some types of conduct than others and differentiates between first time and subsequent offenders.[430]

The International Cybercrime Prevention Act and CCP Trade Secrets Act—both discussed above—proposed a different approach to protect critical infrastructure.[431] They would have each created a new statute—§ 1030A—making it a crime to "knowingly cause or attempt to cause damage to a critical infrastructure computer."[432] Section 1030A would have defined "computer" by reference to the CFAA, and "critical infrastructure" as:

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have catastrophic regional or national effects on public health or safety, economic security, or national security, including voter registration databases, voting machines, and other communications systems that manage the election process or report and display results on behalf of State and local governments.[433]

Two elements would have limited the scope of § 1030A. First, the conduct would have had to occur "during and in relation to a felony violation" of the CFAA.[434] Second, the conduct would have had to result in "substantial impairment" of "the operation of the critical infrastructure computer" or "the critical infrastructure associated with such computer."[435] In other words, § 1030A would have demanded a tighter nexus between the conduct and the critical infrastructure than the Protecting Critical Infrastructure Act of 2021: simply obtaining information without authorization would have been insufficient.[436] Rather, some kind of "substantial impairment" of the computer or the critical infrastructure would have been required.[437] The penalties under § 1030A would also have differed from those proposed in the Protecting Critical Infrastructure Act.[438] In addition to fines, the proposed statute would have authorized up to twenty years of imprisonment on top of the penalty for the underlying CFAA violation.[439] Further, the proposed § 1030A would generally have required this sentence to be served consecutively.[440]

---

[430] *See supra* Section "Remedies and Penalties."

[431] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[432] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[433] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[434] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[435] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021). Section 1030A would also have covered attempts resulting in these conditions.

[436] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[437] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[438] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[439] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

[440] International Cybercrime Prevention Act, S. 2139, 117th Cong. § 5 (2021); CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 305 (2021).

Doxing and Swatting

As noted above, there are a number of ways that doxing and swatting may run afoul of preexisting federal criminal statutes.[441] Several bills introduced in the 117th Congress would have created new statutes more directly aimed at such conduct.[442] With respect to swatting, the Preserving Safe Communities by Ending Swatting Act of 2021 would have expanded the federal hoax statute (18 U.S.C. § 1038) to criminalize engaging "in any conduct with intent to convey false or misleading information" by "using the mail or any facility or means of interstate or foreign commerce, under circumstances where such information may reasonably be expected to cause an emergency response and the information indicates that conduct has taken, is taking, or will take place that constitutes a crime under State or Federal law or endangers public health or safety or the health or safety of any person."[443]

Several bills introduced in the 117th Congress appeared aimed at further criminalizing doxing.[444] At least two of these bills focused on amending 18 U.S.C. § 119—which prohibits making restricted information about certain federal officials and personnel publicly available.[445] One bill would have increased the penalties from up to five years of imprisonment to up to ten years.[446] Another would have expanded the definition of "covered person" protected by § 119 to include an "election official, poll worker, or an election volunteer in connection with an election for a Federal office."[447] A third bill—the Public Servant Anti-Intimidation Act of 2022—took a different approach.[448] It would have created a new statute criminalizing the act of knowingly publishing on the internet or "otherwise mak[ing] publicly available" certain personal information of public servants or their immediate family members.[449] The bill defined public servants to include the President, Members of Congress, and officers or employees of the Executive, Judicial, or Legislative branch.[450] The bill defined personal information to include "home address, home phone number, personal cell phone number, Social Security Number, or other personal identification number."[451]

[441] *See supra* Section "Swatting, Doxing, Cyberstalking, and Cyber Harassment."

[442] *E.g.*, A bill to protect Federal judges, Federal prosecutors, and Federal law enforcement officers from violence and doxing, S. 2247, 117th Cong. (2021); Public Servant Anti-Intimidation Act of 2022, H.R. 8962, 117th Cong. (2022).

[443] Preserving Safe Communities by Ending Swatting Act of 2021, H.R. 4523 § 2 (2021).

[444]Although not a criminal law, in 2022 Congress enacted the Daniel Anderl Judicial Security and Privacy Act of 2022 as part of the National Defense Authorization Act for 2023, which created a privacy law that appears aimed at minimizing the amount of data available online about federal judges and certain family members. *See generally* Daniel Anderl Judicial Security and Privacy Act of 2022, Pub. L. No. 117-263, 136 Stat. 2395.

[445] *See supra* Section "Swatting, Doxing, Cyberstalking, and Cyber Harassment."

[446] A bill to increase the penalties for making personal information about a Federal law enforcement officer or other Federal officer available to the public, S. 2248, 117th Cong. (2021).

[447] Election Worker Protection Act of 2022, S.4920, 117th Cong. § 8 (2022).

[448] Public Servant Anti-Intimidation Act of 2022, H.R. 8962, 117th Cong. (2022).

[449] *Id.* § 2.

[450] *Id.*

[451] *Id.*

Laws that prohibit the transmission of information or restrict speech could raise First Amendment questions to the extent they imposed content-based restrictions on speech.[452] A number of CRS products discuss First Amendment issues that may be relevant to legislating in this space.[453]

The Insider Threat

Many of the highest-profile cybercrime incidents have involved outsiders: for example, hackers who debilitated Colonial Pipeline with ransomware,[454] individuals who added malicious code to a SolarWinds software program used by the government and others,[455] and a computer engineer who conducted a DDoS attack against Boston Children's Hospital.[456] Computers may also be abused by *insiders*, however—those who are permitted or even expected to access a computer in certain circumstances.[457] A quintessential example is the rogue employee who has access to sensitive or confidential information on a computer by virtue of their employment, but who uses that access to misappropriate or disclose that information.[458]

The applicability of the CFAA to insiders such as rogue employees long divided federal courts.[459] As discussed in more detail above, some federal courts have taken the view that the CFAA is "best understood as an anti-intrusion statute and not as a 'misappropriation statute.'"[460] With respect to insiders, these courts generally applied CFAA liability only to those who were "authorized to access only certain data or files" but accessed "unauthorized data or files."[461] For example, these courts may have interpreted the CFAA to apply to a rogue employee authorized *only* to access Database A, who then accessed information in Database B. But they likely would not have construed the CFAA as applicable to a rogue employee authorized to access Database A for limited purposes, if that employee instead accessed Database A for other purposes. In contrast, prior to the Supreme Court's decision in *Van Buren v. United States*, other federal courts might

[452] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011) (noting that "the creation and dissemination of information are speech within the meaning of the First Amendment"). For instance, in one case a federal court examined a state law prohibiting the publishing of certain identifying information about various government employees with "intent to harm or intimidate." Sheehan v. Gregoire, 272 F. Supp. 2d 1135 (W.D. Wash. 2003). The court concluded that the statute was overbroad and violated the First Amendment, because it "punishes the communication of truthful lawfully-obtained, publicly-available information," "is content-based and ... does not serve a compelling state interest or state interest of the highest order," and does "not regulate true threats or any other proscribable mode of speech." *Id.* at 1150.

[453] *E.g.* CRS In Focus IF12308, *Free Speech: When and Why Content-Based Laws Are Presumptively Unconstitutional*, by Victoria L. Killion; CRS In Focus IF11072, *The First Amendment: Categories of Speech*, by Victoria L. Killion.

[454] *See* Press Release, U.S. Dep't of Just., Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (Jun. 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (attributing attack to group known as DarkSide).

[455] *See* Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack ("Hackers believed to be directed by the Russian intelligence service, the SVR, used that routine software update to slip malicious code into Orion's software and then used it as a vehicle for a massive cyberattack against America.").

[456] *Gottesfeld*, 18 F.4th at 4; Nate Raymond, *Massachusetts man gets 10 years in prison for hospital cyberattack*, REUTERS (Jan. 10, 2019), https://www.reuters.com/article/us-massachusetts-cyber/massachusetts-man-gets-10-years-in-prison-for-hospital-cyberattack-idUSKCN1P42J8.

[457] *See generally* S. REP. No. 104-357, at 9 (1996) (describing computer misconduct by insiders in relation to CFAA).

[458] CRS Legal Sidebar LSB10616, *Van Buren v. United States: Supreme Court Holds Accessing Information on a Computer for Unauthorized Purposes Not Federal Crime*, by Peter G. Berris.

[459] *Id.*; *see supra* Section "Without Authorization and Exceeds Authorized Access."

[460] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1196 (9th Cir. 2022) (quoting United States v. Nosal (*Nosal I*), 676 F.3d 854, 857–58 (9th Cir. 2012)).

[461] *Nosal I*, 676 F.3d at 856–57.

have included both types of rogue employee within their broader interpretation of the CFAA, where "the concept of 'exceeds authorized access' [could] include exceeding the purposes for which access is 'authorized.'"[462]

Federal prosecutors had, prior to *Van Buren*, used the CFAA to prosecute insiders, including employees who accessed computers they had authorization to access only for limited purposes but who used them for other purposes.[463] One notable example may be found in the Court's opinion in *Van Buren*, which stemmed from the § 1030(a)(2) prosecution of a police sergeant for using a law enforcement database for personal profit, even though he was authorized only to use the database "for law enforcement purposes."[464] The question of how much the CFAA does, or should, apply to the insider threat punctuated the briefs and oral argument in *Van Buren*.[465] For example, at oral argument, Justice Alito asked whether a narrow reading of the CFAA would leave inadequate protection against insiders such as government employees or "the person in the fraud detection section of a bank" who might use their access to sensitive information for nefarious purposes.[466]

Following *Van Buren*, the CFAA reaches insider conduct if it involves the use of a computer or information on a computer that the insider has *no* right to access.[467] However, *Van Buren* clarifies that the CFAA does not extend to insider threats where the insider obtains information he is permitted to access, even if he does so for impermissible purposes.[468] In the context of the rogue employee, for instance, if he is authorized to obtain his employer's business records for an official purpose such as billing, he will not violate the CFAA if he instead obtains them to sell to a competitor or foreign government.[469]

Such conduct could still have adverse consequences. Most obviously, the individual may be terminated—which happened to the defendant in *Van Buren*.[470] In addition, state laws such as

---

[462] United States v. John, 597 F.3d 263, 272 (5th Cir. 2010), *abrogated by* Van Buren v. United States, 210 L. Ed. 2d 26, 141 S. Ct. 1648 (2021).

[463] *E.g.*, *Van Buren*, 141 S. Ct. 1648.

[464] *Id.* at 1652.

[465] *See*, *e.g.*, Brief for Petitioner at 24, *Van Buren*, 141 S. Ct. 1648 (No. 19-783) (arguing that the only "'inside' hacking" that should be covered by the CFAA are instances where an insider such as an employee accesses computers or portions of computers they are "categorically forbid[den]" from accessing); Brief of Amicus Curiae Digital Justice Foundation In Support of Affirmance at 8, *Van Buren*, 141 S. Ct. 1648 (No. 19-783) (arguing for an agency theory of access where unauthorized access can reach insiders when there is "*ipso facto* terminat[ion of] the agency relationship" and therefore entitlement to access a system); Transcript of Oral Argument at 7, *Van Buren*, 141 S. Ct. 1648 (No. 19-783) [hereinafter "*Van Buren* Transcript"] (question by Roberts, C.J.) ("Just to make sure I have your interpretation correct ... if a bank has a policy barring employees from accessing Facebook, and an employee exceeds her authorized access and would be covered if she goes onto Facebook, but it wouldn't be a violation if she used that access to look up customers' Social Security numbers to sell them to a third party, right?"); *Van Buren* Transcript, *supra*, at 11 (question of Thomas, J.) (asking hypothetical about authorization under CFAA where car rental company employee has "access to the GPS" but improperly uses it "to follow a spouse" rather than to "determine the location of a car that may be missing"); *Van Buren* Transcript, *supra*, at 26 (question of Kavanaugh, J.) (asking what statutes would apply to "government employees or healthcare company employees who have access to very sensitive personal information, then disclose it").

[466] *Van Buren* Transcript, *supra* note 465, at 14.

[467] *Van Buren*, 141 S. Ct. at 1652 ("This provision covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend.").

[468] *Id.* ("It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them.").

[469] *Id.*

[470] *Van Buren* Transcript, *supra* note 465, at 25 (statement of Jeffrey L. Fisher, Esq.) ("[R]emember, my client himself has already lost his job.... ").

those governing trade secrets could conceivably apply.[471] At the federal level, various statutes might be relevant depending on the nature of the conduct and information.[472] Espionage statutes protect certain classified material and defense information, for example.[473] Alternatively, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) limits disclosure of "protected health information."[474] As discussed above, federal criminal law prohibits the theft of trade secrets.[475] Also, if the misappropriation of information involves the internet and a scheme to defraud—interpreted by courts to include depriving someone of money or property by "dishonest methods" such as trickery or deceit—it could implicate the federal wire fraud statute.[476] Not all data misappropriation by an insider will necessarily involve such motives or information subject to specific protections as a trade secret, defense information, protected health information, or under another statute.[477]

To the extent there is a gap such that certain aspects of the insider threat are not covered by federal law, Congress might consider whether legislation is needed to address the insider threat. Recent proposals examining specific aspects of this threat include the Safeguarding American Innovation Act and the Keep America Secure Act from the 117th and 116th Congresses, both of which focused on certain categories of insiders with access to government data.[478]

Another approach may be found in the CCP Trade Secrets Act from the 117th Congress.[479] Among other things, the bill would have redefined the phrase "exceeds authorized access" in the CFAA more broadly than the current definition as interpreted by the Court in *Van Buren*.[480] One definition of "exceeds authorized access" under the CCP Trade Secrets Act was "to access a computer with authorization and thereby to knowingly obtain information from such computer that the accessor is not entitled to obtain."[481] The current definition in the CFAA uses the phrase

[471] *E.g.*, TEX. CIV. PRAC. & REM. CODE ANN. §§ 134A.001–134A.008 (West); CONN. GEN. STAT. ANN. §§ 35-50–35-58 (West).

[472] For example, if military personnel obtain classified information through unauthorized computer use, they may run afoul of the Uniform Code of Military Justice. *E.g.*, 10 U.S.C. § 923, Art. 123 (prohibiting, among other things, "intentionally access[ing] a Government computer, with an unauthorized purpose, and thereby obtain[ing] classified or other protected information from any Government computer").

[473] *E.g.*, 18 U.S.C. §§ 793, 794, 798.

[474] *See generally* CRS Legal Sidebar LSB10797, *Protection of Health Information Under HIPAA and the FTC Act: A Comparison*, by Chris D. Linebaugh and Edward C. Liu.

[475] *See supra* Section "Data Theft."

[476] *See supra* Section "Other Electronic Fraud."

[477] The possibility of a gap in this space appears to be a concern of at least some practitioners following *Van Buren*. *E.g.*, Ambrose V. McCall, *Employers Should No Longer Rely on Their Policies Alone to Support a Computer Fraud and Abuse Act Claim Against Current or Former Employees*, EMPLOYMENT LAW OBSERVER (Jun. 8, 2021), https://www.employmentlawobserver.com/employers-should-no-longer-rely-on-their-policies-cfaa-scotus-van-buren-ruling (counseling that employers who want CFAA coverage and federal law protections and remedies "should consider having their senior managers, IT and HR directors, and in-house and external counsel meet and work together to implement a system of contractual, policy, *and* technological boundaries and terms that limit or deactivate access by current and former employees to an employer's digital assets, networks, and computer and software systems"). As described previously, the CFAA also provides for civil remedies. *See supra* Section "Remedies and Penalties." So although *Van Buren* involved a criminal application of the CFAA, its interpretation of the CFAA governs civil applications of the statute as well. *See, e.g.*, Pable v. Chicago Transit Auth., No. 19-CV-7868, 2022 WL 2802320, at *1 (N.D. Ill. July 18, 2022) (concluding in light of *Van Buren* that an employee did not exceed authorized access as required to be civilly liable under the CFAA when he "misused his authorized access for an improper purpose").

[478] Safeguarding American Innovation Act, S. 1351, 117th Cong. (2021); Keep America Secure Act, H.R. 8309, 116th Cong. Title II, Subtitle A, § 205 (2020).

[479] CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 306 (2021).

[480] *Id.*

[481] *Id.*

"not entitled *so* to obtain."[482] The omission of the word "so" in the CCP Trade Secrets Act would have been potentially significant because the word was key to the Court's holding in *Van Buren*.[483] The Court interpreted "so" as a word that refers back to the preceding text in a manner that explains the method by which the information must be obtained.[484] Thus, the Court held that "[t]he phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access."[485] In other words, the word "so" was integral to the Court's textual conclusion that to exceed authorized access under the CFAA, a computer user must access information that he is not authorized to access at all.[486] By omitting the word "so," the CCP Trade Secrets Act seemingly would have broadened insider liability—presumably covering instances where an individual obtained information for unauthorized purposes.[487] The definition of "exceeds authorized access" in the CCP Trade Secrets Act included a second category of conduct: "knowingly obtain[ing] any information from such computer for a purpose that is prohibited by the computer owner."[488] This definition too would have marked a departure from *Van Buren*, since it would permit CFAA prosecution in instances where an individual was authorized to access a computer but did so for improper purposes. In other words, the bill seemed intended to target the category of insider threat that the *Van Buren* Court excluded from the current CFAA.[489]

The CCP Trade Secrets Act would have clarified that an individual would not exceed authorized access by violating a term of service on a public website, but the bill seemed to permit CFAA liability based on other contractual limitations (such as employer computer-use policies).[490] To the extent that would have been the case, the CCP Trade Secrets Act might have raised some additional questions presented in *Van Buren* that the Court ultimately did not resolve.[491] For instance, if criminal liability under the CFAA hinges on compliance with lengthy contracts that few read, then it could be argued that the CFAA would not "define . . . criminal offense[s] [under the statute] with sufficient definiteness that ordinary people can understand what conduct is prohibited" as required for a criminal statute to avoid constitutional vagueness concerns under the Due Process Clause.[492] Some courts echoed such vagueness concerns in adopting a narrow interpretation of the CFAA.[493] In *United States v. Drew*—which involved a CFAA prosecution of an adult who violated the terms of service of the social media site MySpace as part of a cyberbully scheme—a federal district court concluded that the CFAA would be unconstitutionally vague if "any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of

[482] 18 U.S.C. § 1030(e)(6).

[483] Van Buren v. United States, 210 L. Ed. 2d 26, 141 S. Ct. 1648, 1654–55 (2021).

[484] *Id.* at 1655.

[485] *Id.*

[486] *Id.*

[487] That said, other changes to the definition of "exceeds authorized access" in the bill would likely require further statutory analysis by an interpreting court—for example, the CCP Trade Secrets Act's inclusion of a *mens rea* requirement in the definition of "exceeds authorized access."

[488] CCP Trade Secrets Act, S. 1245, 117th Cong. Title III, § 306 (2021).

[489] *See Van Buren*, 141 S. Ct. at 1652 ("It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them.").

[490] CCP Trade Secrets Act, S. 1245, 117th Cong. (2021), Title III, § 306.

[491] *See Van Buren*, 141 S. Ct. at 1661 (concluding that because the CFAA's text compelled holding, neither the rule of lenity or canon of constitutional avoidance were "in play").

[492] Kolender v. Lawson, 461 U.S. 352, 357 (1983).

[493] *E.g.*, United States v. Nosal *(Nosal I)*, 676 F.3d 854, 859–62 (9th Cir. 2012).

authorization."[494] Relatedly, the *Drew* court expressed concern that using contractual violations "as the basis for [a CFAA] crime" effectively "makes the website owner-in essence-the party who ultimately defines the criminal conduct."[495] According to some, that would not only contribute to the possibility of arbitrary enforcement,[496] but it would also make behavior that is traditionally the domain of state tort and contract claims the subject of federal criminal law.[497]

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer

[494] United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009).

[495] *Id.* at 465.

[496] For a discussion of this issue—albeit in the context of terms of service—see generally *id.* at 466–67.

[497] *See, e.g.*, JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 524 (S.D.N.Y. 2013) ("Indeed, the broad reading of 'exceeds authorized access' has breathtaking implications" and "would federalize, and potentially subject to federal criminal law, quotidian abuses by employees that have historically been the sole ambit of state employment and criminal law."); Matwyshyn & Pell *supra* note footnote 367, at 487 ("As explained by one of us in prior work, when pedestrian breach of contract claims potentially become CFAA civil claims and chargeable as criminal offenses under the CFAA, the traditional boundary between contract law and criminal law is violated.").