CAN JAILBREAKING PUT YOU IN JAIL, BROKE?

Trace H. Jackson[*]

Abstract

Most Americans own at least one "smart device." These include smartphones and video game consoles. Device manufacturers limit an owner's use of his smart device through both licensing agreements and technological measures. While the public largely ignores licensing agreements, the technological measures actively prevent an owner from using his device in whatever manner he sees fit, despite the fact that he *owns* the device. This prevention has led people to develop methods to circumvent these technological measures. These methods are device-dependent and include "jailbreaking" (iPhones), "modding" (video game consoles), and "rooting" (Androids).

This Note explores whether jailbreak developers or jailbreak users violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Congress passed the Act in response to the threat of criminals hacking into government or bank computers. As such, it makes little sense to apply the Act to people who want more freedom of use of their devices. A large number of smart device users employ some form of jailbreaking. The fact that the government could prosecute them under an anti-hacking statute for violating the licensing agreement for their devices, paves the way for many new and terrifying prosecutions.

* J.D. (University of Florida, 2016); Editor in Chief, *Florida Law Review*. I would like to thank Samanta Franchim, Wes Hevia, Kimberly A. Kelley, Matt Lastinger, Miranda Moore, Cate Parsley, Steven Palmer, Justin Senior, Cayman Weimer, Michael Woods, our staff editors, Lisa Caldwell and Angelia Forder, and especially my Executive Managing Editor, Megan Testerman, for their outstanding work on this piece. I would also like to thank Kim Bouchard-Chaimowiz, Jared Gaylord, and Maris Snell for their helpful comments and emotional support.

INTRODUCTION

A "smart device" is a device that can connect to other devices or networks and operate "interactively and somewhat autonomously."[1] Examples of smart devices include video game consoles and smartphones. To operate interactively and autonomously, these devices typically come with software called an operating system (OS). For example, Microsoft's Xbox One video game console comes with a variant of Microsoft's Windows 8,[2] and Apple's iPhone runs iOS.[3]

While these OSes primarily enable the operations of the device, they also limit the activities of the user. For example, iOS does not permit the user to install any applications (apps) besides those that Apple has officially approved for use in its App Store.[4] Additionally, Android phones have a feature called "wireless tethering," which allows owners to use their phones as Wi-Fi hotspots for other devices, such as laptops.[5] However, telecom companies such as Verizon forced Android developers to restrict this ability so that only customers who paid extra for the feature could use it.[6]

Device manufacturers have this level of control over end use of the device because of their control over the OS. They have this control because the user does not *own* most of the software she uses; she licenses it.[7] This lack of ownership allows the developer more control over the device's use because the user must typically agree to an End User Licensing Agreement (EULA)[8] of the software to install it. EULAs serve as clickwrap agreements, permitting developers to impose their own sets

---

1. *See Wi-Fi Connectivity Increases Purchase Likelihood for Smart Home Devices*, WI-FI ALLIANCE, http://www.wi-fi.org/news-events/newsroom/wi-fi-connectivity-increases-purchase-likelihood-for-smart-home-devices (last visited Sept. 10, 2015).

2. Dina Bass, *Xbox One Has Not One, but Three Operating Systems*, BLOOMBERG (Nov. 22, 2013, 7:55 AM), http://www.bloomberg.com/news/2013-11-22/xbox-one-has-not-one-but-three-operating-systems.html.

3. *iOS 9*, APPLE, https://www.apple.com/ios/ (last visited Sept. 10, 2015).

4. *See* Sam Costello, *Can I Get iPhone Apps Without iTunes?*, ABOUTTECH http://ipod.about.com/od/iphoneapps/f/iphone-apps-without-itunes.htm (last visited Sept. 10, 2015).

5. *See* Brian Nadel, *Wi-Fi Tethering 101: Use a Smartphone as a Mobile Hotspot*, COMPUTERWORLD (Nov. 4, 2011, 7:00 AM), http://www.computerworld.com/article/2499772/mobile-wireless/wi-fi-tethering-101-use-a-smartphone-as-a-mobile-hotspot.html.

6. A settlement with the FCC has since ended this practice. *See* Marguerite Reardon, *What Verizon's FCC Tethering Settlement Means to You (FAQ)*, CNET (Aug. 2, 2012 10:53 AM), http://www.cnet.com/news/what-verizons-fcc-tethering-settlement-means-to-you-faq/.

7. 1 MICHAEL D. SCOTT ET AL., SCOTT ON MULTIMEDIA LAW § 23.01 (3d ed. Supp. 2014).

8. EULA is the common term when dealing with software. Some developers also refer to licensing agreements as "terms of use" or "terms of service" interchangeably, though they have a more nuanced meaning.

of laws on the use of their software.[9] Despite their perceived unconscionability, courts have upheld clickwrap agreements as valid contracts between the developer and user.[10] Thus, circumvention of EULAs may be tantamount to breach of contract.[11]

Because manufacturers bundle smart devices with the software that makes the devices operable (OSes), EULAs limit the use of smart devices.[12] This notion is fundamentally at odds with the average person's concept of ownership of his own devices. One of the most basic sticks in the property rights bundle is the ability to use the property in any manner that the owner sees fit, provided that the use does not negatively affect others.[13] Due to the EULAs, that is not the case for smart devices.

As a result, many enterprising users of these devices seek a way to circumvent the limitations that the manufacturers impose on smart devices. They accomplish this circumvention through methods known as "modding" (video game consoles), "jailbreaking" (iPhones), and "rooting" (Androids).[14] Although there is a technical distinction between each of these, and although some Android developers permit rooting, this Note refers to them collectively as "jailbreaking." Jailbreaking restores freedom of use to the users[15] and allows them to make changes to their devices, such as changing the OS,[16] developing and installing unauthorized apps,[17] unlocking smartphones to switch carriers,[18] and even altering the function of the device.[19] Naturally, the ability to make these alterations makes jailbreaking very popular.[20]

---

9. *See, e.g.*, Ruth Okediji, *Givers, Takers and Other Kinds of Users: A Fair Use Doctrine for Cyberspace*, 53 FLA. L. REV. 107, 165 (2001).

10. *See, e.g.*, I.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002). *But see* Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91 (3d Cir. 1991) (holding that shrinkwrap licenses are not binding).

11. Complaint at 53, Sony Comput. Entm't Am. LLC v. Hotz, No. 3:11CV00167 (N.D. Cal. Jan. 11, 2011) [hereinafter Sony Complaint].

12. PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS § 1.07 cmt. a (AM. LAW INST. 2010).

13. 63C AM. JUR. 2D *Property* § 31 (2014).

14. See Joshua A.T. Fairfield, *Nexus Crystals: Crystallizing Limits on Contractual Control of Virtual Worlds*, 38 WM. MITCHELL L. REV. 43, 45 (2011).

15. For a brief technical explanation, see *infra* Section II.B.

16. *See, e.g.*, CYANOGENMOD, http://www.cyanogenmod.org/ (last visited Sept. 10, 2015).

17. *See* Ali Hassan Mahdi, *Jailbreak Apps and Tweaks*, IPHONE HACKS (Sept. 8, 2015), http://www.iphonehacks.com/jailbreak-apps.

18. It was necessary to jailbreak the phone to unlock it prior to the passage of the Unlocking Consumer Choice and Wireless Competition Act, Pub. L. No. 113-144 (2014).

19. *See, e.g.*, Alan Henry, *Turn a $99 Nook into a Fully Fledged Android Tablet in Four Easy Steps*, LIFEHACKER (Feb. 29, 2012, 8:00 AM), http://lifehacker.com/5889158/turn-a-99-nook-into-a-fully-fledged-android-tablet-in-four-easy-steps.

20. One jailbreaking program for iOS 6 was installed more than seven million times within six days after its release in February of 2013. Anthony Wing Kosner, *What 7 Million Jailbreaks Are Saying. Is Apple Listening?*, FORBES (Feb. 10, 2013, 8:06 AM),

However, most device developers do not approve of such alterations—otherwise they would not have such restrictive EULAs in the first place. While the developers have some technological deterrents against jailbreakers,[21] they also seek legal deterrents. This is in part because of the ease of legal intimidation in the jailbreaking community. Most users who develop jailbreaks do so as a hobby with no expectation of payment.[22] As a result, if a device developer threatens to sue a jailbreak developer, the jailbreak developer would likely prefer to settle or acquiesce to a cease-and-desist demand, rather than fight it in court, because the jailbreak developer receives minimal financial gain. Thus, the jailbreaking community is one where legal bullying works extremely well, and the lawyer who can throw in as many allegations as she can without violating Rule 11's proscription of unmeritorious pleadings[23] will likely be successful.[24]

This Note discusses the civil and criminal liability of a jailbreak user and a jailbreak developer under one of these possible allegations: a violation of the Computer Fraud and Abuse Act (CFAA).[25] Part I provides the necessary background for the discussion, including an explanation of its disjointed legislative history and the relevant technical explanation of jailbreaking. Part II applies the CFAA to the act of jailbreaking to conclude that using a jailbreak may violate the CFAA, but developing one almost certainly does.

---

http://www.forbes.com/sites/anthonykosner/2013/02/10/what-7-million-jailbreaks-are-saying-is-apple-listening/. One popular video game console modding website, ps3hax.net, had over 380,000 registered users as of June 30, 2016, many of whom were actively involved in the developments of mods for the PlayStation 3. *See PS3Hax Network – Playstation 3 and Playstation 4 Hacks and Mods*, PS3HAX, http://www.ps3hax.net/forum.php (last visited June 30, 2016). The number of *downloads* of the mods is likely substantially higher.

21. *See generally* PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 382–85 (4th ed. 2011) (describing several technological protection measures).

22. *See A Beginners Guide to Developing for a Jailbroken iOS Platform*, PRIYAONTECH (Jan. 12, 2012), http://www.priyaontech.com/2012/01/a-beginners-guide-to-developing-for-a-jailbroken-ios-platform/. *But see* Ian Shapira, *Once the Hobby of Tech Geeks, iPhone Jailbreaking Now a Lucrative Industry*, WASH. POST (Apr. 7, 2011), http://www.washingtonpost.com/business/economy/once-the-hobby-of-tech-geeks-iphone-jailbreaking-now-a-lucrative-industry/2011/04/01/AFBJ0VpC_story.html.

23. FED. R. CIV. P. 11(b).

24. *See, e.g.*, Sony Complaint, *supra* note 11. This is not in any way to allege that Sony engaged in the aforementioned tactic of legal bullying. This is merely to give an example of a corporation employing as many legal theories as possible against an underrepresented defendant who had no financial incentive to fight and who ultimately settled.

25. 18 U.S.C. § 1030 (2012).

I. BACKGROUND

Analyzing whether jailbreaking violates the CFAA requires a brief explanation of two key background concepts. First, this Part discusses the legislative history of the CFAA, which originally sought to protect government and bank computers but which now covers *any* computer in interstate commerce (i.e., nearly all of them). Second, it provides a small technical explanation of jailbreaking and modding.

A. *The Computer Fraud and Abuse Act*

The CFAA, codified at 18 U.S.C. § 1030, is a statute aimed primarily at computer hacking activities. Congress enacted the law as a proactive measure against some foreseeable computer-related crimes that might have escaped prosecution under the then-existing giants of federal criminal law: mail fraud and wire fraud.[26] It amended the previous version of 18 U.S.C. § 1030, which was part of the Comprehensive Crime Control Act of 1984.[27] The original CFAA proscribed "knowingly access[ing] a computer without [or exceeding] authorization"[28] and the following three activities: (1) obtaining information that the federal government determined needed protection against public release to protect interests of national defense or foreign relations;[29] (2) obtaining financial information from a bank;[30] or (3) using, modifying, destroying, or disclosing information, or preventing authorized use of a computer used by or on behalf of the federal government.[31]

Aside from an additional provision for prohibiting conspiracy to commit an offense under the CFAA,[32] the statute prohibited no other conduct. It is important to note that Congress narrowly tailored each of these offenses to protect a strong federal interest. In particular, the first and third offenses in the numbered list above involve attacks upon the federal government itself, while the second offense implicates interstate commerce.[33] Congress also narrowly tailored this statute to ensure an

---

26. *See* H.R. REP. NO. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692. *See generally* OFFICE OF LEGAL EDUCATION, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, PROSECUTING COMPUTER CRIMES 1 (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf [hereinafter CYBERCRIME MANUAL] (examining the federal laws that relate to computer crimes).

27. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. XXI, §§ 2101–2103, 98 Stat. 1837, 2190 (codified as amended at 18 U.S.C. § 1030).

28. 18 U.S.C. § 1030(a)(1) (Supp. II 1984) (amended 1986).

29. *Id.*

30. *Id.* § 1030(a)(2).

31. *Id.* § 1030(a)(3).

32. *Id.* § 1030(b).

33. *See* U.S. CONST. art. I, § 8, cl. 3.

"appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses."[34]

In 1986, Congress added a definition and three new offenses to the CFAA, thus further expanding federal jurisdiction.[35] Congress expanded the class of computers that the statute protected by defining a "federal interest" computer as a computer used by or on behalf of the federal government or financial institutions, or "one of two or more computers used in committing the offense, not all of which are located in the same State."[36] The first new offense paralleled the language found in the wire[37] and mail fraud[38] statutes, thus criminalizing trespassing on a federal interest computer in such a way that furthered a scheme to defraud and that resulted in the trespasser obtaining something of value.[39] The second new offense was accessing a federal interest computer; altering, damaging, or destroying information on that computer; and either causing losses aggregating to over $1000 in a one-year period or interfering with medical care.[40] The final new offense was trafficking passwords either that belonged to a government computer or in such a way as to affect interstate commerce.[41]

These changes came at an interesting time in American legal history. In particular, internet use was in its infancy, and Commerce Clause jurisprudence was at its most liberal.[42] This amendment is important because it allowed the prosecution of one private individual who harmed another private individual, in contrast to the original statute, which required the hacker to harm the government or a bank in order to face prosecution.

The current version of the CFAA expands the definition of a federal interest computer further. In addition to those computers used by financial institutions or the government,[43] the statute protects *any*

34. S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.

35. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (2012)). Interestingly, Congress also changed the *mens rea* requirement in some of the provisions from "knowingly" to "intentionally," as they felt the need to protect people who accidentally stumbled into someone else's data. S. REP. NO. 99-432, at 5, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483.

36. 18 U.S.C. § 1030(e)(2) (Supp. III 1985) (amended 1988).

37. 18 U.S.C. § 1343 (2012).

38. *Id.* § 1341.

39. 18 U.S.C. § 1030(a)(4) (Supp. III 1983) (amended 1988).

40. *Id.* § 1030(a)(5).

41. *Id.* § 1030(a)(6).

42. *See generally* 1 RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW § 4.8 (4th ed. 2007) (discussing the shifting scope of Congress's Commerce Clause power).

43. 18 U.S.C. § 1030(e)(2)(A) (2012).

computer "used in or affecting interstate or foreign commerce or communication."[44] As noted in Section II.A, *infra*, this extremely broad definition covers almost any conceivable computer. This increase in scope makes sense in light of the structure of the modern Internet.[45] Moreover, the range of offenses has dramatically increased from the 1986 version. The two offenses relevant to the jailbreaking analysis are 18 U.S.C. § 1030(a)(2)(C), which proscribes "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtains . . . information from any protected computer,"[46] and § 1030(a)(5)(A), which deals directly with hacking by prohibiting "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer."[47]

B. *Jailbreaking*

This Note considers two types of "hacking": jailbreaking and modding. Although one can consider them the same from a legal standpoint, technically they are different. It is important to understand some of the technical details of each.

Fundamentally, jailbreaking refers to the circumvention of the iPhone's authenticity checks. When a user turns her iPhone on, iOS checks that the OS's components are unchanged from Apple's official version.[48] The primary goal of jailbreaking is to disable these checks by exploiting the system software to load the user's own software onto the phone.[49] This enables users to break out of the "jail" of the limited set of directories on the user's phone to which iOS permits access.[50] Similarly, if a Windows computer only allowed a user to access the user's My Documents folder, then jailbreaking would be analogous to restoring the user's ability to access the entire computer.[51]

---

44. *Id.* § 1030(e)(2)(B).

45. *See, e.g.*, United States v. Lewis, 554 F.3d 208, 210, 215 (1st Cir. 2009) (holding that the intrastate transmission of child pornography over the Internet constituted interstate commerce because the data packets containing the pornography were split up and sent through an uncertain path that likely went out of the state to reach the destination).

46. 18 U.S.C. § 1030(a)(2)(C).

47. *Id.* § 1030(a)(5)(A).

48. *See* Michael K. Cheng, Note, *iPhone Jailbreaking Under the DMCA: Towards a Functionalist Approach in Anti-Circumvention*, 25 BERKELEY TECH. L.J. 215, 222 (2010).

49. *Id.*

50. *See generally iPhone Forensics—A Series #2*, MOBILE DEVICE FORENSICS (Sept. 17, 2008), http://mobileforensics.wordpress.com/2008/09/17/iphone-forensics-a-series-2/ (discussing the technical aspects of jailbreaking an iPhone).

51. *See* Cheng, *supra* note 48, at 222 ("In its default state, the iPhone Software only allows the user to access the file system's '/private/var/mobile/Media' directory.").

The video game console analogue is modding. Mods come in both physical and virtual forms—a user may install a physical "mod chip"[52] or may download a mod program that takes advantage of exploits in the system's security.[53] These mods can serve a variety of functions, including changing the OS entirely, deleting the OS's check that a chosen game is authentic, and restoring root access like the iPhone jailbreak.[54] Functionally and legally, this is equivalent to jailbreaking because both involve exploiting the system in order for a user to transmit his own code, so this Note will refer to both processes as "jailbreaking."

II. JAILBREAKING VIOLATES THE CFAA

The CFAA sets out seven general offenses in subsection (a), provides the criminal punishment factors in subsection (c), and imposes civil liability in subsection (g). The two most relevant subsections to the jailbreaking analysis are (a)(2)(C) and (a)(5)(A). Subsection (a)(2)(C) prohibits gaining unauthorized access or exceeding authorized access to a "protected computer," and using that access to obtain information.[55] Given that merely viewing information qualifies as obtaining it for the purpose of the CFAA,[56] the only issues for proving a violation of (a)(2)(C) are whether smart devices are protected computers and whether jailbreaking them exceeds authorized access. Section II.A establishes that smartphones and video game consoles are protected computers within the meaning of the statute. Section II.B considers whether jailbreaking constitutes "unauthorized access" or "exceeding authorized access" within the meaning of the statute.

Subsection (a)(5)(A) prohibits transmitting a program (like a jailbreak) to a protected computer and, as a result of the transmission, causing damage without authorization.[57] Section II.C of this Note considers whether jailbreaking constitutes "damage" to the computer within the meaning of the statute. Section II.D explores the criminal and

52. *See generally* Jason Rybka, *Modchips—What Are They and Should You Use One?*, ABOUT TECH, http://vgstrategies.about.com/od/faqglossary/a/modchips.htm (last visited Sept. 10, 2015) (illustrating the pros and cons of modding a console).

53. *See, e.g.*, MICHAEL STEIL, 17 MISTAKES MICROSOFT MADE IN THE XBOX SECURITY SYSTEM, http://events.ccc.de/congress/2005/fahrplan/attachments/591-paper_xbox.pdf (describing such possible exploits in the Microsoft Xbox's security system).

54. *See, e.g.*, Patrick Schmid, *Modding the Xbox into the Ultimate Multimedia Center*, TOM'S HARDWARE (May 11, 2004, 11:00 AM), http://www.tomshardware.com/reviews/modding-xbox-ultimate-multimedia-center,807.html.

55. 18 U.S.C. § 1030(a)(2)(C) (2012).

56. S. REP. NO. 99-432, at 6–7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 ("'[O]btaining information' in this context includes mere observation of the data. Actual asportation . . . need not be proved . . . .").

57. 18 U.S.C. § 1030(a)(5)(A).

civil liability based on these offenses.

A. *Smartphones and Video Game Consoles Are Protected Computers*

The first element of any violation of the CFAA is that the "victim" computer must be a protected computer within the meaning of the statute. This means that the device must be both a "computer" and "protected."[58] Subsection 1030(e)(1) defines a computer as "an electronic . . . or other high speed data processing device performing logical, arithmetic, or storage functions."[59] Smart devices fit this definition.

Intuitively, assuming the CFAA's definition of "computer" applies to home computers and laptops, then both video game consoles and smartphones are computers. A home computer has a publicly released OS (e.g., Windows), reads any data format for which the computer has an input mechanism (e.g., the computer can read information from a CD using its CD-ROM drive), and displays that information to a display device (e.g., a monitor or a television).[60] Similarly, a video game console is a specialized computer that has a proprietary OS, reads a proprietary data format (such as cartridges, CDs, or BluRay discs), and displays that data on a television. In a smartphone, the underlying hardware is identical and even more powerful than the hardware on computers when Congress passed the CFAA in 1986.[61]

Courts have agreed that smart devices are computers. The U.S. Court of Appeals for the Eighth Circuit held in *United States v. Kramer*[62] that any device with a "microchip" is a computer.[63] The device in that case was a non-smartphone, the Motorola Razr V3.[64] The court reasoned that given § 1030(e)(1)'s requirement that the device merely process data and perform logical, arithmetic, or storage functions—the functions of a microchip—any device with a microchip must qualify as a computer.[65] The cellphone had a microchip, so it was a computer. The court also recognized how broad this definition could be,[66] and a plain language

58. *Id.* § 1030(e)(1)–(2).

59. *Id.* § 1030(e)(1).

60. *See* Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 169 (2011).

61. *See id.*

62. 631 F.3d 900 (8th Cir. 2011).

63. *See id.* at 901–03. Note that "microchip" is a brand name, like "Kleenex," but the court also discusses electronic data processors generally, which is probably what the court meant.

64. *Id.* at 901.

65. *See id.* at 902.

66. The court quotes Steve Wozniak, cofounder of Apple, as observing that "everything has a computer in it nowadays." *Id.* at 901 (quoting Mark Milian, *Apple's Steve Wozniak: 'We've Lost a Lot of Control,'* CNN (Dec. 8, 2010), http://www.cnn.com/2010/TECH/innovation/

reading of the statute does not admit a narrower definition. A federal court in California also held that video game consoles are computers, at least for the purposes of granting a preliminary injunction.[67] Thus, intuitively and legally, smart devices are computers.

The harder question, however, is whether these devices qualify as *protected* computers. Subsection 1030(e)(2)(B) defines a protected computer as one "used in or affecting interstate . . . commerce."[68] When Congress uses the term "affects interstate commerce," Congress generally means to regulate all activity that it may reach under the commerce power.[69] Therefore, the issue is whether the use of these devices is an activity that Congress has the power to regulate. Under modern Commerce Clause theory, Congress may regulate an activity if it is an economic activity with a substantial effect on interstate commerce.[70] This is true even if the activity is a purely local one that affects interstate commerce only in the aggregate.[71] Both video game consoles and smartphones affect interstate commerce.

Modern video game consoles tend to be connected to the Internet. Services such as Microsoft's Xbox Live and Sony's PlayStation Network allow users to connect with other users over the Internet and, more importantly, to purchase games and other add-ons from the developer's store.[72] These services tend to be subscription-based, so users wishing to log onto a service such as Xbox Live must pay for the privilege of doing so.[73] By purchasing a subscription, users outside of Microsoft's home state of Washington are clearly engaging in interstate commerce.[74] Moreover, even users within Washington affect interstate commerce in

---

12/08/steve.wozniak.computers/); s*ee also* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577–78 (2010) (noting that this definition could include "coffeemakers, microwave ovens, watches, . . . televisions, . . . CDs, DVDs, and other electronic storage devices").

67. *See* Sony Comp. Entm't Am. v. Hotz, No. CV11 000167, 2011 WL 347137 (N.D. Cal. Jan. 27, 2011) (order granting preliminary injunction).

68. 18 U.S.C. § 1030(e)(2) (2012).

69. *See* Stirone v. United States, 361 U.S. 212, 215 (1960) (holding that the term "affecting trade" in the Hobbs Act, 18 U.S.C. § 1951, demonstrates a Congressional intent to "use all the constitutional power Congress has").

70. *See* United States v. Lopez, 514 U.S. 549, 558–59 (1995).

71. *See* Wickard v. Filburn, 317 U.S. 111, 128 (1942).

72. *See, e.g.*, *Xbox 360 Marketplace*, MICROSOFT, http://marketplace.xbox.com/en-US/ (last visited Sept. 14, 2015).

73. *See, e.g.*, *Xbox Live*, MICROSOFT, http://www.xbox.com/en-US/LIVE (last visited Sept. 14, 2015).

74. A 2010 Forbes article estimated that Microsoft made at least $625 million in global sales of Xbox Live subscriptions. Oliver Chiang, *Microsoft's Xbox Live Is Making Boatloads of Money on Virtual Goods*, FORBES (June 17, 2010, 6:15 AM), http://www.forbes.com/sites/velocity/2010/06/17/microsofts-xbox-live-is-making-boatloads-on-virtual-goods/.

the aggregate by purchasing a service from an international company such as Microsoft, thus giving these companies more assets with which to affect interstate commerce.[75]

A harder case may be those console owners who do not purchase a service such as Xbox Live. This accounts for many owners who mod their video game consoles, because most developers require subscribers to update their consoles frequently, and during the updates, the developers impose authenticity checks to ensure that the consoles are not modded.[76] As a result, such console owners would be concerned with connecting their consoles to the Internet, which might sever the link to interstate commerce. Although the console owner in this case would have participated in interstate commerce by purchasing the device, her *use* of it would not affect interstate commerce.

However, a court could still find a link to commerce by analogizing to the rule of *Gonzalez v. Raich*.[77] In *Gonzalez*, the plaintiff sought a declaratory judgment that the Controlled Substances Act (CSA) did not apply to her because she grew marijuana in her backyard for her own medicinal use.[78] She argued that because the marijuana was for her own use and would never enter into interstate commerce, the application of the CSA to her was an unconstitutional overstep of the limitations of the commerce power.[79] This use of marijuana was a purely local, intrastate, noneconomic activity.[80] However, the Supreme Court held that this regulation of the plaintiff's activities was within the commerce power.[81] The Court reasoned that the plaintiff's activities were regulated by a larger, legitimate federal scheme.[82] As a result, even though the regulation "ensnare[d] some purely intrastate activity," the CSA was valid as applied to the plaintiff.[83] The Court seemed concerned with the ease with which even some of the plaintiff's own marijuana might leak out into the market, and that was enough to regulate the plaintiff's

75. Under the Hobbs Act, depletion of assets qualifies as affecting interstate commerce. *See, e.g.*, United States v. Urban, 404 F.3d 754, 762–63 (2005). It follows that increasing assets also qualifies.

76. Adrian Kingsley-Hughes, *Microsoft "Bricked" 360s with "Live" Update*, ZDNET (Nov. 6, 2006, 11:02 PM), http://www.zdnet.com/blog/hardware/microsoft-bricked-360s-with-live-update/137. In the most severe cases, this can render the console inoperable ("bricking" the console).

77. 545 U.S. 1 (2005).

78. *Id.* at 7.

79. *See id.* at 8.

80. The mere use of a video game console is debatably economic, since a video game console has few uses when the user neither connects it to the Internet nor purchases any games for it.

81. *Id.* at 22.

82. *Id.*

83. *Id.*

activities under the CSA.[84]

Video game consoles that are not connected to the Internet are similar. Although using the game consoles without connecting is purely local, a court might find the regulation of such devices to be part of a larger "regulatory scheme" that "could be undercut" if the devices were not regulated (due to the ease with which a user can connect his device to the Internet).[85] However, if a court accepts that interpretation, then it is debatable whether the word "protected" has any meaning within the statute. Courts interpret statutes so that every word has meaning;[86] consequently, a court might reject this interpretation on the basis that it would render the word "protected" meaningless. On the other hand, the term may be merely a "jurisdictional element which would ensure, through case-by-case inquiry, that the [computer] in question affects interstate commerce."[87] On balance, the *Gonzalez* argument seems more applicable to video game consoles because of their potential for connectivity to the Internet (and thus engage in interstate commerce). Thus, the use of both connected and non-connected video game consoles affect interstate commerce and therefore are "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

Smartphones are protected computers, for many of the same reasons given above. Most smartphone owners have a data plan, meaning that the smartphones are connected to the Internet.[88] Some courts have held that merely being connected to the Internet is sufficient to meet the interstate commerce element, finding "that the Internet is an instrumentality [or] channel of interstate commerce,"[89] thus granting Congress the authority to regulate it.[90] For those smartphone users who do not have a data plan, the *Gonzalez* argument above would likely persuade a court that Congress may also regulate these users.

B. *Jailbreaking May Exceed Authorized Access*

Another element for several of the offenses listed within § 1030(a) is access to the protected computer that either is unauthorized or exceeds

84. *Id.*

85. *See* United States v. Lopez, 514 U.S. 549, 561 (1995).

86. *See* Reiter v. Sonotone Corp., 442 U.S. 330, 339 (1979) ("In construing a statute we are obligated to give effect, if possible, to every word Congress used.").

87. *See Lopez*, 514 U.S. at 561.

88. According to a 2013 Nielsen report, ninety-six percent of smartphone owners in the United States have a data plan. NIELSEN, THE MOBILE CONSUMER: A GLOBAL SNAPSHOT 15 (2013), http://www.nielsen.com/content/dam/corporate/uk/en/documents/Mobile-Consumer-Report-2013.pdf.

89. United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006).

90. *See, e.g.*, United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007); *see also* CYBERCRIME MANUAL, *supra* note 26, at 4–5.

authorized access.[91] The CFAA defines "exceeds authorized access" as "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."[92] However, this statutory definition does not alone provide much guidance for the jailbreaking analysis. On one hand, a reasonable interpretation of the statute as applied to the jailbreaking problem is that the jailbreaker (user or developer) accesses his device with authorization because he bought it. On the other hand, because the word "entitled" implies a superior authority that sets limits on access, it follows that this authority is the same one that grants "authorization."[93] There are three competing views on the scope of this authorization: a broad interpretation that covers violations of terms of service agreements, such as EULAs; a narrow interpretation that excludes them;[94] and a failure of interpretation that declares the term "unauthorized" void for vagueness.[95]

The U.S. Courts of Appeals for the First, Fifth, and Eleventh Circuits subscribe to a broad interpretation of culpable unauthorized access.[96] For example, in *EF Cultural Travel BV v. Explorica, Inc.*,[97] the defendant created a scraper program to glean information from the plaintiff's website.[98] In doing so, the defendant used confidential information that he was privy to as a result of his previous employment with the plaintiff.[99] This violated his confidentiality agreement with the plaintiff, which was enough for the court to find that the defendant's access to the plaintiff's website was unauthorized.[100] The court reasoned that the defendant

91. 18 U.S.C. §1030(a) (2012).

92. *Id.* § 1030(e)(6) (emphasis added).

93. Courts occasionally conflate "unauthorized access" with "exceeding authorized access." However, this might be harmless, as some courts, such as the *Drew* and *Nosal* courts, see a violation of a terms of service agreement that exceeds authorized access as terminating the right to access a computer (thus rendering further access unauthorized). *See infra* text accompanying notes 103–37.

94. Robert D. Sowell, Comment, *Misuse of Information Under the Computer Fraud and Abuse Act: On What Side of the Circuit Split Will the Second and Third Circuits Wind Up?*, 66 FLA. L. REV. 1747, 1748 (2012).

95. *See* Kerr, *supra* note 66, at 1572.

96. *See* Sowell, *supra* note 94, at 1751. Notably, the U.S. Court of Appeals for the Seventh Circuit has also used the broad interpretation, but it did so in the context of an employee violating his employer's computer use policy. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006); Sowell, *supra* note 94, at 1752. The Seventh Circuit used agency law, rather than contract law, to find unauthorized access, so its analysis is irrelevant to jailbreaking, where there is no agent. *Id*. at 420; Sowell, *supra* note 94, at 1752.

97. 274 F.3d 577 (1st Cir. 2001).

98. *Id.* at 580–81.

99. *Id.* at 582.

100. *Id.* at 582–83.

entered into the confidentiality agreement voluntarily, and that the defendant knew he violated the confidentiality agreement by providing the necessary information for the scraper.[101] Thus, according to this broad interpretation, any knowing violation of a voluntary agreement between the party providing a service and the party accessing the service constitutes unauthorized access for the purposes of the CFAA.[102]

The U.S. Courts of Appeals for the Fourth and Ninth Circuits use a narrower interpretation of "unauthorized access."[103] In *United States v. Nosal*,[104] the defendant asked employees of a company to violate their computer use policy that forbade the dissemination of confidential information from the company's computers, and the Government charged the defendant with violating the CFAA under an accomplice liability theory.[105] The en banc Ninth Circuit held that a mere violation of a terms of service agreement could not rise to the level of unauthorized access for the purposes of the CFAA.[106] The court based its reasoning both on statutory interpretation and on legislative intent, writing that the broad interpretation would "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute," despite Congress's original intent to create an anti-hacking statute.[107]

According to the court, the statutory term "without authorization" applies to "*outside* hackers," while the term "exceeds authorized access" applies to "*inside* hackers."[108] This construction avoids the problem that the court saw with the broad interpretation: it allowed criminal liability to attach to "the vagaries of private policies that are lengthy, opaque, subject to change, and seldom read."[109] The court cited examples of innocuous activity that would be illegal under the broad interpretation, such as sending a family member an email from the user's work email (although calling that same family member from a work phone would not be a criminal act).[110] In the internet context, a minor using Google or a

101. *Id.* at 583.

102. It is important to note that this holding does not appear to rest on the *type* of agreement. Thus, the fact that the agreement in this case was a confidentiality agreement, rather than a mere terms of service agreement, is irrelevant. *See* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (holding that an intentional violation of America Online's terms of service for the purpose of harvesting email addresses constituted unauthorized access to America Online's services).

103. Sowell, *supra* note 94, at 1752.

104. 676 F.3d 854 (9th Cir. 2012) (en banc).

105. *Id.* at 856.

106. *See id*. at 863.

107. *Id.* at 857–58.

108. *Id.* at 858.

109. *Id.* at 860.

110. *Id.* The court appears to be invoking the "avoiding absurdity" canon of construction with this example. *See generally* John F. Manning, *The Absurdity Doctrine*, 116 HARV. L. REV.

user lying about his age on eHarmony would carry criminal liability.[111] While the Government insisted that it would not target lesser violations, the court reasoned that it could not support a construction that would allow for unfettered discretion of the police.[112] The court concluded that the CFAA prohibited "improper 'access' of computer information[,] not . . . misuse or misappropriation,"[113] and that any other construction would fail to take into consideration the "effect on millions of ordinary citizens" that a broad interpretation would have.[114]

Whereas the *Nosal* court used a statutory construction that avoided unconstitutional vagueness, one district court has held this portion of the CFAA void for vagueness. In *United States v. Drew*,[115] the defendant, a middle school girl, created a fake profile on the social networking website MySpace pretending to be an older boy to bully a fellow student.[116] The defendant added a picture of the boy to the MySpace profile without the boy's permission, violating MySpace's terms of service.[117] The terms of service stated that the user was "only authorized to use the Services . . . if [the user] *agree[d] to* abide by all applicable laws and to this Agreement."[118] The jury convicted her of a misdemeanor violation of § 1030(a)(2)(C).[119]

The defendant then filed a motion for a judgment of acquittal, and the district court granted the motion, on the grounds that the term "without authorization" was void for vagueness.[120] After reasoning that the basis of the conviction was a violation of the MySpace terms of service, the court held that the term "without authorization" in the statute failed both prongs of the void for vagueness test: the term failed to give fair notice to a citizen wishing to comport her behavior with the requirements of the law,[121] and it gave unfettered discretion to the police.[122]

2387, 2388 (2003) ("[J]udges may deviate from even the clearest statutory text when a given application would otherwise produce 'absurd' results.").

111. *Id.* at 861. In the court's words, "describing yourself as 'tall, dark, and handsome' when you're actually short and homely, will earn you a handsome orange jumpsuit." *Id.* at 862.

112. *Id.*; *see also* text accompanying notes 113–37.

113. *Nosal*, 676 F.3d at 863 (quoting Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010)).

114. *Id.* at 862.

115. 259 F.R.D. 449 (C.D. Cal. 2009).

116. *Id.* at 452.

117. *Id.*

118. *Id.* at 466.

119. *Id.* at 453.

120. *Id.* at 467–68.

121. *Id.* at 464–66; *see also* Papachristou v. City of Jacksonville, 405 U.S. 156, 162–66 (1972) (explicating the fair notice prong of the void for vagueness test).

122. *Drew*, 259 F.R.D. at 466–67; *see also* Kolender v. Lawson, 461 U.S. 352, 357–58 (describing the police guidelines prong of the void for vagueness test).

The court provided four reasons why the statutory language relating to authorization failed to give fair notice. First, the court reasoned that the acceptance of the terms of service amounted to a clickwrap contract, and while a reasonable person might anticipate civil liability for a breach of contract, he would never anticipate criminal penalties.[123] Second, the court reasoned that the terms of service were vague because they did not establish whether a violation of *any* term within the terms of service rendered any access unauthorized, or whether only certain violations rose to that level.[124] The court equated a violation that would result in the termination of a user's account with a violation that would render access unauthorized.[125] However, based on the terms of service, the court could not determine whether violations of terms such as prohibitions on "gambling" or "disclosing your password to a third party" would result in the termination of the user's account.[126] Thus, the terms of service agreement itself was too vague to be used as the basis for applying the CFAA.

Third, and similarly, the court was very uncomfortable allowing the owner of the website to define criminal conduct.[127] The owner of the website was under no obligation to draft terms of service with any clarity.[128] Website owners can alter the terms of service with no input from or notice to its users.[129] For example, MySpace's terms of service allowed MySpace to determine what was "prohibited content" at its "sole discretion."[130] Therefore, the terms of service provided no actual notice of culpable conduct to users. Finally, even if the terms of service were sufficiently definite, many terms of service agreements, including that of MySpace, contain an arbitration requirement for any dispute arising from the terms of service.[131] The court thought it was unclear whether a finding of unauthorized access required a finding of a breach during arbitration.[132]

The court also held that the statute failed to give minimal guidelines for law enforcement.[133] The court reasoned that the terms of service

123. *Drew*, 259 F.R.D. at 464.

124. *Id.*

125. *Id.* at 464–65.

126. *Id.*

127. *Id.* at 465.

128. *Id.*

129. *Id.*

130. *Id.* (quoting *Myspace.com Terms of Use Agreement*, MYSPACE (Feb. 28, 2008), http://www.myspace.com/misc/terms.html [https://web.archive.org/web/20041205011200/http://www.myspace.com/misc/terms.html]).

131. *See id.*

132. *Id.*

133. *Id.* at 466.

agreement was so broad in scope that the breach of many provisions would result in prosecution.[134] For example, minor breaches such as a user lying about her age to create a profile or posting a picture of a person without his consent could qualify as a breach that results in prosecution, even if that breach did not result in any "actual loss or . . . violation of privacy interests."[135] While the Government argued that the statute had a sufficient limiting factor in its *mens rea* requirement, interpreting this provision of the CFAA to require wrongful intent, the court disagreed that this imposed any significant requirement.[136] The court held that even such an interpretation would result in a "standardless sweep," permitting law enforcement "to pursue their personal predilections."[137]

Each of these three interpretations of the term "authorized access"—the broad interpretation that includes mere terms of service, the narrow interpretation that excludes them, and the nihilistic interpretation that the statute is void for vagueness—provides separate answers for the question of whether jailbreaking constitutes unauthorized access. However, because each interpretation is based on authorization being determined by a terms of service agreement, an important question is whether jailbreaking actually violates the terms of service agreement of the device. The remainder of this Section examines two such agreements: one for the Sony PlayStation 4 and one for the iPhone. Generally, *creating* a jailbreak based on modified code seems to be a violation of the terms of service, while manufacturers vary their terms regarding *using* one.

The software licensing agreement for the Sony PlayStation 4 (PS4 Agreement) seems to ban creating and using mods.[138] On the subject of creating mods, Section 2 of the agreement—entitled "Restrictions"—states: "You may not . . . modify, patch, [or] adapt . . . System Software. You may not reverse engineer, decompile or disassemble System Software, create System Software derivative works, or attempt to create System Software source code from its object code."[139] A plain language reading of that section suggests that the act of creating a mod violates the PS4 Agreement. To create the mod, a modder must reverse engineer the "System Software" to determine how the software interacts with the

134. *Id.*

135. *See id.* at 466–67.

136. *Id.* at 467.

137. *Id.* (quoting Kolender v. Lawson, 461 U.S. 352, 358 (1983)).

138. *See PlayStation 4 System Software License Agreement*, SONY COMPUT. ENTM'T INC. (2015), http://www.scei.co.jp/ps4-eula/ps4_eula_en.html [hereinafter *PS4 Agreement*] (describing restrictions on the use of System Software). Recall that modding is the video game console term for jailbreaking. *See supra* text accompanying note 14.

139. *PS4 Agreement*, *supra* note 138.

hardware of the PlayStation 4 and create a workable OS. Additionally, the mod software itself is likely a derivative work.[140]

The installation of a mod also violates the PS4 Agreement. Section 2 continues:

> You may not (i) use any unauthorized . . . or modified hardware or software with System Software; (ii) use tools to bypass, disable or circumvent any PS4 system encryption, security or authentication mechanism; (iii) reinstall earlier versions of the System Software ("downgrading"); . . . (v) use any hardware or software to cause System Software to accept or use unauthorized, illegal or pirated software or hardware . . . .[141]

This is an exceptionally restrictive set of terms. The PS4 Agreement prohibits using the type of mod that installs a new OS on the PlayStation 4.[142] It also prohibits more basic mods. For example, a user cannot bypass the system authentication mechanism, which merely checks for the presence of authentic software.[143] A user cannot circumvent the PlayStation 4's mechanism for ensuring that only Sony-approved software is used on the system.[144] Finally, a user cannot "downgrade" to a previous version of Sony's own OS.[145] Thus, the PlayStation 4 prohibits both creating and using mods.

In contrast, Apple seems to focus on the developers of jailbreak OS software. In Subsection 2(d) of its iOS 8.1 Software License Agreement, Apple states: "You may not, *and you agree not to or enable others to*, copy . . . , decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, or create derivative works of the iOS Software . . . ."[146] This is functionally identical to the language in the PS4

---

140. *See* 4 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 12:9 (West 2015); s*ee also, e.g.*, Liu v. Price Waterhouse LLP, 302 F.3d 749, 754 (7th Cir. 2002) (finding an updated version of software to be a derivative work).

141. *PS4 Agreement*, *supra* note 138.

142. *See id.*

143. *See id.*

144. *See id.* This is mostly an anti-piracy measure. Rather than purchasing a PlayStation 4 game, the user could go to a website, download an image of the game, burn it onto a system disc (here, a BluRay disc), and insert that disc into the PlayStation 4. However, the system has technological protection measures to ensure that this does not happen and circumventing those violates the PS4 Agreement. Nevertheless, such circumvention is the goal of many of the most popular mods.

145. *See id.* This is because many mods are made to circumvent certain versions of the system's OS. Sony updates the OS in part to block these mods, so Sony does not want users downgrading back to an older version that they could circumvent.

146. *iOS Software License Agreement*, APPLE, http://images.apple.com/legal/sla/docs/iOS81.pdf (last visited Nov. 16, 2015) [hereinafter *iOS Agreement*] (emphasis added).

Agreement proscribing the creation of a mod. Additionally, one may interpret the language as prohibiting the deletion of the stock iOS software (i.e., installing a jailbreak) because the agreement prohibits disassembling the software.[147] However, one of the canons of contract interpretation is to give technical terms their technical meaning.[148] In the computer software context, "disassemble refers to analyzing executable programs.[149] Given the other computing terms surrounding "disassemble," such as "decompiling," this seems like the appropriate interpretation. Therefore, while installing a jailbreak does not seem to violate the licensing agreement, creating one probably does, and thus may be a violation of the CFAA.

Taking these two licensing agreements to be prototypical, it seems that the act of creating a jailbreak would exceed a user's authorized access (or render it unauthorized) under the broad interpretation of "authorized access" within the CFAA, consequently making jailbreak development a violation of § 1030(a)(2)(C) in jurisdictions that subscribe to the broad interpretation. On the other hand, the legality of *installing* a jailbreak depends on whether the EULA of the device in question forbids doing so. However, all that prevents an otherwise-legal jailbreak installation from becoming illegal is the whim of the developer.[150] That is the problem that the Ninth Circuit and the *Drew* court saw in the broad interpretation of the authorization requirement.

Notably, most licensing agreements include choice of law and venue provisions that favor California and the Ninth Circuit.[151] Both the Ninth Circuit's narrow interpretation[152] and the *Drew* court's finding of vagueness[153] suggest that a mere violation of the terms of service agreement does not rise to the level of a CFAA violation. While a developer-plaintiff or the Government likely could not prevail at all under the *Drew* court's rule, they might have a chance under the Ninth Circuit's rule. In particular, a developer-plaintiff or the Government would need to

147. *See id.*

148. *See* RESTATEMENT (SECOND) OF CONTRACTS § 202(3)(b) (AM. LAW INST. 1981).

149. *See* Benjamin Schwarz, Saumya Debray & Gregory Andrews, *Disassembly of Executable Code Revisited*, 9 PROC. WORKING CONF. ON REVERSE ENGINEERING 45, 45 (2002), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1173063.

150. An open question is whether an element of a CFAA prosecution is that the terms of service be a valid contract. In other words, might unconscionability be an affirmative defense?

151. *See, e.g.*, *iOS Agreement*, *supra* note 146, § 12 (stating that the iOS Agreement is "governed by and construed in accordance with the laws of the State of California, excluding its conflict of law principles"); *PS4 Agreement*, *supra* note 138, § 10 (stating that the PS4 Agreement is "governed by, construed and interpreted in accordance with the laws of the State of California except for its conflict of law rules").

152. *See supra* text accompanying notes 103–14.

153. *See supra* text accompanying notes 115–37.

argue that the act of developing or installing a jailbreak rises above a mere terms of service agreement violation. They might argue that developing a jailbreak is more similar to the "inside hack[ing]" that the Ninth Circuit believed "exceeds authorized access."[154] However, without further guidance from the Ninth Circuit, the rule seems to require more than a violation of a terms of service agreement, so jailbreaking is likely not a violation of § 1030(a)(2)(C) in the Ninth Circuit.

C. *Jailbreaking Damages Smart Devices*

Subsection 1030(a)(5) prohibits three acts with subtle differences. The first is "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer."[155] The second is "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage."[156] The third is "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss."[157] Section II.B covers the issue of whether the access is authorized.[158] Section II.C focuses on the first of these offenses. The primary issue is whether jailbreaking constitutes "damage." If it does, then the jailbreaker could be liable under (a)(5)(A).

The CFAA broadly defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[159] As the *Cybercrime Manual* points out, this definition encompasses any act that "causes data or information to be deleted or changed" or that "changes the way a computer is instructed to operate."[160] This language is simultaneously vague and overbroad. For example, if Alicia sends a revised memo to Bob, who inadvertently saves the revised memo and overwrites the original, then Alicia has caused data or information to be

154. United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (emphasis omitted).

155. 18 U.S.C. § 1030(a)(5)(A) (2012).

156. *Id.* § 1030(a)(5)(B).

157. *Id.* § 1030(a)(5)(C).

158. Subsection 1030(a)(5)(A) is unique within the CFAA because the unauthorized act is causing damage, rather than accessing an unauthorized computer. This implies that some damage may be authorized. However, it seems logical that if a court finds accessing the phone to execute a jailbreak to be unauthorized, then the subsequent damage must also be unauthorized. The other subsections require that the access itself be unauthorized. While the broad interpretation of the access element essentially establishes an equivalence between "exceeds authorized access" and "unauthorized access," the Ninth Circuit sees a distinction based on "inside hackers" and "outside hackers," respectively. *See Nosal*, 676 F.3d at 858 (emphasis omitted). Based on this interpretation, jailbreaking would not violate (5)(B) and (5)(C) because the "hacker" is inside.

159. 18 U.S.C. § 1030(e)(8).

160. CYBERCRIME MANUAL, *supra* note 26, at 39.

deleted or changed. Alicia would not be culpable under the CFAA because this was not Bob's intention; however, Bob still caused damage.

Jailbreaking clearly causes damage under this definition. In the smartphone context, where the user replaces her OS (or makes changes to it), she has clearly impaired the "availability of . . . a program."[161] The user intentionally overwrote the OS. Intuitively, choosing to alter one's own device should not constitute damage. The legislative history of the CFAA supports this idea. The definition of damage is intentionally broad to include "the types of harm against which people should be protected."[162] However, Congress did not design the CFAA to protect people from themselves. The government could only prosecute jailbreakers (and developers could only sue them) to protect the *developers*. Deleting the developer's software likely constitutes damage to it. The developer must be the party that the statute protects because it is the developer who originally denied access to the user.[163]

The argument in the video game console context is similar. As stated in the Introduction, most console mods involve changing the console so that it can play games that it was not meant to play, such as games that the user downloaded illegally. This usually involves deleting authenticity checks,[164] which changes how the "computer is instructed to operate."[165] Thus, modding a video game console also causes damage within the statutory meaning.

Assuming that this broad interpretation of "damage" is correct, then the second issue involves the specific *actus reus* and *mens rea* of the defendant. There are two types of offenses within § 1030(a)(5): either the defendant "knowingly causes the transmission of a program, information, code, or command,"[166] or the defendant "intentionally accesses a protected computer."[167]

The jailbreak developer can only be liable for the first act under (a)(5)(A). By publishing the jailbreak on a public website, he would know or be substantially certain that someone would download it. Moreover, he would know that the downloader's purpose would be to install the jailbreak—to cause damage. He therefore knowingly put it on his website, hoping that people would download it and intending that the download damage the protected computer. While the jailbreak developer

---

161. *See* 18 U.S.C. § 1030(e)(8).

162. S. REP. NO. 104-357, at 11 (1996).

163. Otherwise, this logic, taken to its extreme, would suggest that a user could never delete *any* applications.

164. *See supra* Section I.B.

165. *See* CYBERCRIME MANUAL, *supra* note 26, at 39.

166. 18 U.S.C. § 1030(a)(5)(A).

167. *Id.* § 1030(a)(5)(B)–(C).

could argue that he did not know *which particular* protected computer his conduct would damage, that seems irrelevant for the purposes of this statute.[168] Thus, the developer would be liable under (a)(5)(A).

Arguably, the user would also be liable under (a)(5)(A). Assuming she did not download the jailbreak accidentally, she caused its transmission by clicking the download button. Moreover, she must have transmitted it from the device where she downloaded the jailbreak onto the device to be jailbroken, intending to cause damage. However, (a)(5)(A) seems more concerned with defendants such as the jailbreak developer.

D. *Civil Liability and Criminal Punishment*

Merely committing one of the offenses in 18 U.S.C. § 1030(a) is not enough to trigger civil liability or criminal punishment. This Section explores the other factors required to punish a jailbreaker.

The CFAA establishes civil liability in § 1030(g):

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief . . . only if the conduct involves [one] of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).[169]

The first subclause grants relief if the offense caused "loss to [one] or more persons during any [one]-year period . . . aggregating at least $5,000 in value."[170] The CFAA defines "loss" broadly 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 [or] cost incurred."[171] Such loss would be easiest to prove in the video game console modding context. Many console developers release updates designed to play whack-a-mole with modders.[172] If the developer could show that the cost of developing such a patch exceeded $5000 in value, including the standard hourly rate for employees' time,[173]

---

168. If the statute required the defendant to know which specific computer he was targeting, then that would exclude hackers who post malware online for any visitor to a website to download.

169. 18 U.S.C. § 1030(g) (footnoted omitted).

170. *See id.* § 1030(c)(4)(A)(i)(I).

171. *Id.* § 1030(e)(11).

172. *See, e.g.*, Rob Crossley, *Nintendo Blocks 3DS NINJHAX Hack with Firmware Update*, GAMESPOT (Dec. 11, 2014), http://www.gamespot.com/articles/nintendo-blocks-3ds-ninjhax-hack-with-firmware-upd/1100-6424146/ (describing a situation where software update blocked users from playing unlicensed games).

173. *See* United States v. Sablan, 92 F.3d 865, 869–70 (9th Cir. 1996); CYBERCRIME MANUAL, *supra* note 26, at 43.

then the developer would meet this requirement. In the criminal context, the prosecution would meet it as well, since the statute only requires the loss to "*any* victim."[174] However, it seems unlikely that the mere *use* of a jailbreak would rise to this level.

The second subclause provides a remedy if the offense modified or impaired the "medical examination, diagnosis, treatment, or care of [one] or more individuals."[175] Doctors frequently use tablets[176] in medical examinations.[177] If the jailbroken tablet somehow interfered with the examination (e.g., the tablet lost its capability to access the Internet at a critical time during the examination), then a plaintiff may be able to add a CFAA claim to his medical malpractice claim. However, as the example demonstrates, this seems to be extremely unlikely.

The fourth and fifth subclauses are the most disturbing. They create the possibility of compensatory or injunctive relief if the offense created a "threat to public health or safety" or "affect[ed] a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security."[178] This is concerning because the National Security Agency (NSA)—through a government program such as PRISM—may have installed "back door[s]" on devices such as smartphones for surveillance purposes.[179] Additionally, many service providers store information such as text message logs, which the gvernment can subpoena.[180] Suppose that a person developed a jailbreak to cripple the ability of the NSA and service providers to intercept or store messages. That gives rise to a number of questions that are beyond the scope of this Note. First, could the government argue that the jailbreaker created a threat to public safety, particularly if she released the jailbreak? Second, could someone who used the jailbreak be considered to have affected a computer used by the

174. 18 U.S.C. § 1030(e)(11) (emphasis added).

175. *Id.* § 1030(c)(4)(A)(i)(II).

176. While this Note has not yet discussed tablets, since they are essentially larger smartphones (though not exempt from the Digital Millennium Copyright Act (DMCA)), they can likely be treated in the same way as smartphones for the purposes of the CFAA.

177. Kevin Bostic, *As Medicine Goes Digital, Apple's iPad Is Top Choice Among Doctors*, APPLEINSIDER (May 31, 2013, 9:37 AM), http://appleinsider.com/articles/13/05/31/as-medicine-goes-digital-apples-ipad-is-top-choice-among-doctors (claiming that fifty-one percent of office-based doctors use a mobile device for medical reference and that fifty-nine percent of doctors integrate tablets into their operations).

178. 18 U.S.C. § 1030(c)(4)(A)(i)(IV)–(V).

179. *See Privacy Scandal: NSA Can Spy on Smart Phone Data*, SPIEGEL ONLINE (Sept. 7, 2013, 6:00 PM), http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html; Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

180. 18 U.S.C. § 2703(b).

government in furtherance of justice? If not, could she fall within this subclause if she was under investigation and jailbroke her phone to prevent surveillance? Would she have to know she was under surveillance for subclause (V) to apply? Finally, if the answer to any one of those questions is yes, could the gvernment get an injunction to force such a jailbreaker to install surveillance software on her own phone? That clearly raises a Fourth Amendment issue.

The CFAA establishes criminal liability in § 1030(c). The level of punishment depends on the section of the CFAA used to convict the defendant. If the defendant were convicted under (a)(2)(C), then the defendant would only be punished if one of three criteria were met: (1) the defendant developed or used the jailbreak for "commercial advantage or private financial gain";[181] (2) the defendant developed or used the jailbreak "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State;"[182] or (3) "the value of the information obtained [through the jailbreak] exceeds $5,000."[183] Each of these three provisions could apply. For example, if the defendant, a jailbreak developer, included on his website a link to his PayPal, that might trigger the first provision. Similarly, because modding a video game console is not an exception to the Digital Millennium Copyright Act (DMCA), installing a mod might be done in furtherance of a criminal act (violating the DMCA). Finally, while a user might not obtain more than $5000 in installing the jailbreak, the developer might obtain this much money (through advertising, for example).

If the defendant were convicted under (a)(5)(A), then the first use or development of a jailbreak is likely a misdemeanor,[184] unless a court finds that the use or development of a jailbreak results in a loss of at least $5000, in which case the use or development of a jailbreak would be a felony.[185] That determination is the same as the one that a court would need to make in connection with a conviction under (a)(2)(C). Lastly, regardless of which clause is used to target jailbreakers (users or developers), the second time a jailbreaker is convicted for modifying her own device, she is a felon.[186]

CONCLUSION

Jailbreak development and use likely violates 18 U.S.C. § 1030(a)(5)(A). In jurisdictions that hold that a violation of a terms of

181. *Id.* § 1030(c)(2)(B)(i).

182. *Id.* § 1030(c)(2)(B)(ii).

183. *Id.* § 1030(c)(2)(B)(iii).

184. *See id.* § 1030(c)(4)(G)(i).

185. *See id.* § 1030(c)(4)(B)(i).

186. See *id.* § 1030(c)(2)(A), for a conviction under (a)(2)(C). See *id.* § 1030(c)(4)(C)(i), for a conviction under (a)(5)(A).

service agreement or EULA constitutes exceeding authorized access (or rendering future access unauthorized), development also violates 18 U.S.C. § 1030(a)(2)(C). The legality of jailbreaking depends on the tolerance of the manufacturers in such jurisdictions. However, in the Ninth Circuit, where most litigation involving jailbreaking takes place, it seems that jailbreaking would not violate the CFAA.

Given the legislative history of the CFAA, it does not seem that legislating compliance with a terms of service agreement was the goal of the Act. The CFAA was designed to prevent hackers from gaining access to and acquiring information from computers worthy of protection—those of banks and the government itself. However, it seems that by being clumsy with wording and drafting in terms overbroad in scope, Congress has made it a crime for a user to make unacceptable alterations to the user's own device. Given that the CFAA is a virtual analogue of a trespass statute, this is illogical. As the Ninth Circuit and the *Drew* court noted, allowing private entities to define the criminal law with no definiteness requirements could lead to disastrous results. Congress should rewrite the CFAA to adopt the Ninth Circuit's holding that violating a terms of use agreement does not exceed authorized access, at least if the user owns the device. Thus, device manufacturers could deal with jailbreakers privately, and users could be left to their own devices.