Fordham Law Review

Volume 86 | Issue 2 Article 16

2017

Reevaluating the Computer Fraud and Abuse Act: Amending the Statute to Explicitly Address the Cloud

Amanda B. Gottlieb
Fordham University School of Law

REEVALUATING THE COMPUTER FRAUD AND ABUSE ACT: AMENDING THE STATUTE TO EXPLICITLY ADDRESS THE CLOUD

*Amanda B. Gottlieb**

Cloud-computing systems from companies such as Apple, Google, and Microsoft can run on multiple types of devices, such as laptops, tablets, and smartphones, and can sync data across these devices. Many consumers initially invest in several of these products, then later choose to upgrade and purchase the newest models, resulting in the same cloud-computing accounts syncing to a variety of gadgets.

This Note seeks to answer the question whether an individual violates the Computer Fraud and Abuse Act (CFAA), an antihacking statute passed by Congress in 1986, when she accesses data that is on a device only because it is stored in the cloud, after receiving authorization to use the device for other purposes like internet browsing. To do so, this Note first traces the CFAA's history and explores the four approaches to interpreting authorization under the Act adopted by different courts of appeals. Next, this Note argues that although the CFAA is widely interpreted in the employment context, courts can still analyze an individual's access to data on a cloud-computing system through the CFAA lens as the Act is currently written. This Note then applies each CFAA approach to a scenario involving the cloud.

Under the current interpretations of authorization, instances where an individual harmlessly accesses the cloud data of another user could be classified as hacking and a violation of this federal statute. As such, this Note demonstrates that all of the current interpretations of the CFAA are too broad because they could result in this nonsensical outcome. This Note accordingly proposes an amendment to the CFAA specifically addressing user access to data on the cloud. Such an amendment would eliminate the unusual result of innocuous cloud-computing users being deemed hackers under federal law.

* J.D. Candidate, 2018, Fordham University School of Law; B.A., 2012, University of Michigan. I would like to thank Professor Joel Reidenberg and the editors and staff of the *Fordham Law Review* for their assistance and guidance in publishing my Note. I would also like to thank Matt and my family for their endless love and support. Without their encouragement, none of this would be possible.

INTRODUCTION

On July 1, 2016, Edward Majerczyk was charged with felony computer hacking related to a phishing scheme that gave him illegal access to over 300 iCloud and Gmail accounts, including some belonging to celebrities.[1] The

1. *See* Press Release, U.S. Attorney's Office for the Cent. Dist. of Cal., Illinois Man Charged with Hacking Apple iCloud and Gmail Accounts Belonging to More Than 300 People, Including Many Celebrities (July 1, 2016), https://www.justice.gov/usao-cdca/pr/illinois-man-charged-hacking-apple-icloud-and-gmail-accounts-belonging-more-300-people [https://perma.cc/KS7Z-DE73].

charges against Majerczyk stemmed from an investigation by the FBI into leaked pictures of female celebrities.[2] His scheme involved sending emails to victims that appeared to be from security accounts of internet service providers.[3] The victims were directed to a website where they were prompted with a fraudulent login screen, which collected their usernames and passwords.[4] Majerczyk ultimately pleaded guilty to a felony violation of the Computer Fraud and Abuse Act (CFAA).[5]

Majerczyk's story is a prototypical example of a person actively trying to steal information from others—an act typically thought of as hacking in violation of the CFAA.[6] Imagine instead that a friend, significant other, or coworker innocently asks to borrow your tablet to have internet access for a few days as a substitute for her computer, which is being repaired. You may not think twice about letting her borrow your device. Today's technology, however, presents a unique problem that you might easily overlook: because many commonly used devices can be synced through a cloud-computing system ("the cloud"),[7] whomever you lent your device to now has continuous access to your email, messages, photos, calendar, and other personal information that may be stored in the cloud.[8] For example, loaning someone your iPad may be indistinguishable from loaning them your iPhone because any data stored on the cloud may be accessible through both devices.[9] Any actions taken on your smartphone could automatically sync to the tablet you lent out, due to real-time updates of your data on the cloud.[10]

In the hypothetical situation above, though you gave this person access to your device to browse the internet, you likely did not intend to give her access to your entire cloud account as well. As technology continues to advance and people upgrade to the latest electronics, it is not hard to imagine other situations in which your unlocked device, connected to the cloud, falls into the hands of someone else. For instance, this issue could arise if an individual decides to sell a phone on eBay (or another similar site) or donate it to a charity to be repurposed without thoroughly restoring the device to factory settings. The operative question thus becomes, is the inadvertent access of

2. *Id.*
3. *Id.*
4. *Id.*
5. *See id.*; *see also* 18 U.S.C. § 1030 (2012). The CFAA was passed by Congress in 1986 as an antihacking statute and has been amended over the years to encompass many types of computer crimes. *See infra* Part I.B. When referring to § 1030 of the CFAA, this Note is referencing the portion of the U.S. Code where the Act is codified unless otherwise indicated.
6. *See* 18 U.S.C. § 1030; *see also infra* Part I.B (providing an overview of the CFAA). Majerczyk is classified as an outside hacker as opposed to an inside hacker. *See infra* notes 76–83 and accompanying text (explaining inside and outside hackers). When an individual violates the CFAA, she has acted "without authorization" or "exceeds authorized access" under the statute. *See infra* Part I.B (discussing these terms, which are found within the text of the CFAA).
7. *See infra* Part I.A (explaining the function and purpose of these systems). The terms "cloud-computing system" and "the cloud" will be used interchangeably throughout this Note.
8. This hypothetical situation is referenced throughout this Note.
9. *See infra* Part I.A (explaining the function and purpose of cloud-computing systems).
10. *See infra* Part I.A (discussing how the cloud seamlessly syncs devices with one another).

your personal information by a third party through the cloud, when given general access to your device, a violation of the CFAA?[11]

Despite no mention of a traditional computer in the hypothetical situation, the CFAA is still the applicable statute. Under the CFAA definition of "computer,"[12] the list of items that qualify as computers is expansive and continuously growing as technology advances. The definition currently includes any device with a microchip, such as smartphones, tablets, and laptops.[13] However, while courts have recognized that newly developed devices may fall within the CFAA's purview,[14] the law in practice has not been able to keep up with new innovations, and the cloud currently exists in a sort of legal purgatory.[15] Although courts would likely determine that the cloud falls within the ambit of the CFAA,[16] courts face the difficult challenge of determining how the CFAA in practice would apply to situations involving unauthorized access to data on a cloud system.[17]

Congress passed the CFAA in 1986 to address the growing problem of computer crimes but, despite the numerous amendments to the Act, none reflect the unique problems posed by the cloud.[18] Further complicating the statute's application to this present-day issue, the CFAA has been interpreted mostly in the employment context and there is a circuit split regarding how

11. Cloud-computing systems could include Apple's iCloud, Google's Google Drive, or Microsoft's OneDrive. Data on cloud-computing systems have been analyzed in terms of the Fourth Amendment and the government's access to information stored in the cloud. *See, e.g.*, William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1211 (2010) (analyzing government access to the cloud under the Fourth Amendment). This Note takes a different approach by analyzing access to information on the cloud through the CFAA. Lawsuits involving the cloud are likely to become more common as individuals increasingly rely on cloud-computing systems to store their data. *See id.* at 1204; *see also infra* Part I.A. The question this Note seeks to resolve is important because the cloud is not specifically mentioned in the text of the CFAA. Computer access under this statute is an ambiguous area of the law, which should be clarified before an innocuous computer user is unfairly classified as a hacker for accessing another person's cloud data. *See infra* Part III.

12. The CFAA defines "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1) (2012).

13. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577–78 (2010); *see also* 18 U.S.C. § 1030(e)(1); United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011) (affirming an expansive definition of "computer" and holding that an ordinary cell phone was a computer under the definition found in the CFAA). In fact, Steve Wozniak, cofounder of Apple, has said that "[e]verything has a computer in it nowadays." Mark Milian, *Apple's Steve Wozniak: We've Lost a Lot of Control*, CNN (Dec. 8, 2010, 12:16 PM), http://www.cnn.com/2010/TECH/innovation/12/08/steve.wozniak.computers/index.html [https://perma.cc/DU35-HNDN].

14. *See Kramer*, 631 F.3d at 903–04.

15. *See infra* Part III.

16. Christopher Satti, *A Call to (Cyber) Arms: Applicable Statutes and Suggested Courses of Action for the Celebrity iCloud Hacking Scandal*, 34 QUINNIPIAC L. REV. 561, 582 (2016).

17. *See* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 371 (2013).

18. *See infra* Part I.B. The cloud is unique because it can seamlessly sync many devices with one other and quickly pass information between devices. *See infra* Part I.A.

the words "exceeds authorized access," included in § 1030(a)(2) of the Act, are interpreted.[19]

This Note argues that all of the current interpretations of authorization under the CFAA adopted by the circuit courts to determine whether a computer user is a hacker are inadequate when applied to situations involving the cloud, like the hypothetical outlined above.[20] This Note ultimately proposes an amendment to the CFAA to specifically address the cloud. Part I of this Note discusses the background of cloud computing and the CFAA. Part II then analyzes the circuit split that currently exists in this area of the law and then applies the different approaches to the hypothetical involving the cloud outlined at the beginning of this Note.[21] Part III concludes that the interpretations of authorization that evolved from the circuit courts in the employment context can be applied to this new situation but that all of them would classify an innocuous cloud-computing user as a hacker, which is an inequitable result. Part III also suggests an amendment to the CFAA to specifically address cloud computing because, as a matter of common sense, an individual in this hypothetical situation should not be considered a hacker.

I. AN OVERVIEW: UNDERSTANDING THE CLOUD AND THE CFAA BEFORE THEY INTERSECT

Tracing the intersection of the cloud and the CFAA necessitates a brief overview of their historical origins and functional mechanisms. Part I.A discusses the definition of cloud computing and analyzes the function and purpose of cloud-computing systems. Part I.B then examines the evolution of the CFAA into the expansive criminal statute that it is today.

A. Cloud Computing: Definition, Function, and Purpose

Although there is no single definition of "cloud computing," many scholars cite the definition established by the National Institute for Standards and Technology (NIST).[22] According to the NIST, "cloud computing is a model

19. Much of the case law surrounding the CFAA revolves around issues in the employment context. Usually an employer brings charges against a former employee for "exceed[ing] authorized access" when utilizing the company computer system. *See infra* Part II (explaining the various interpretations of the CFAA adopted by the circuit courts).

20. The scenario where someone comes into contact with another person's personal information through a cloud-computing system may touch upon a variety of areas that the law protects in addition to hacking, such as interception and privacy. This Note looks at whether the action is considered hacking and focuses solely on whether an individual has violated the CFAA. In the interest of concision, this Note does not address applications of the Electronic Communications Privacy Act (ECPA) to the operative hypothetical. Due to the expansive reach of the CFAA, it controls almost every interaction with a computer and is the "primary federal authority protecting computing technology from intrusions." Jonathan S. Keim, *Updating the Computer Fraud and Abuse Act*, ENGAGE, Oct. 2015, at 31, 32; *see also infra* Parts I.B, II. In addition, the statute that later became the CFAA was the first federal statute to criminalize unauthorized access to computers. *See infra* notes 48–49 and accompanying text.

21. *See supra* note 8 and accompanying text.

22. *See* William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 BUS. LAW. 237, 237 & n.1 (2010); Kesan

for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[23] Cloud computing has also been described as "a multi-faceted technological phenomenon in which important aspects of computing . . . move from local systems to more efficient, outsourced systems where third parties provide aggregated computational resources and services on an as-needed basis from remote locations."[24]

Much of society's daily digital consumption occurs through the cloud.[25] Today, people often communicate through social networking sites and electronic messaging, such as email, text messaging, and other instant messaging applications that use the internet.[26] Smartphones now allow users to access email, calendars, websites, documents, and PDFs on the go.[27] The cloud also enables users to run applications and store data over the internet instead of on a specific computer, which makes a personal computer's hard drive unnecessary for saving information.[28] So long as a user has a device connected to the cloud, the information can be accessed from anywhere on a variety of devices over the internet.[29]

Cloud-computing service providers "operate a group of computer servers that are connected to each other and function as a single 'cloud' of resources."[30] Cloud computing offers consumers flexibility and access to cloud storage for their information without a large financial investment.[31] Cloud providers are able to keep costs down because customers are often sharing a "pool of computing resources."[32] The customer is usually unaware of exactly where her data is being stored or what the service infrastructure looks like.[33]

---

et al., *supra* note 17, at 356. The NIST has statutory responsibilities under the Federal Information Security Management Act of 2002 and is responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets. *See* PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUBLICATION 800-145, THE NIST DEFINITION OF CLOUD COMPUTING § 1.1 (2011).

23. MELL & GRANCE, *supra* note 22, § 2.

24. Urs Gasser, *Cloud Innovation and the Law: Issues, Approaches, and Interplay* 2 (Berkman Ctr. for Internet & Soc'y at Harvard Univ., Research Publication No. 2014-7, 2014), http://ssrn.com/abstract=2410271 [https://perma.cc/GP6E-SVLC].

25. *See* Kesan et al., *supra* note 17, at 341.

26. *See id.* at 350.

27. *See id.* at 351.

28. *See* Robison, *supra* note 11, at 1199–1200.

29. *See id.* at 1202; *see also* Simon Bradshaw et al., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services* 5 (Sch. of Law at Queen Mary Univ. of London, Research Paper No. 63/2010, 2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 [https://perma.cc/UC47-53BM].

30. Robison, *supra* note 11, at 1199.

31. *See* Bradshaw et al., *supra* note 29, at 1.

32. *Id.* at 5.

33. *See id.* at 3.

On June 6, 2011, Apple introduced the world to its version of the cloud, iCloud, for the first time.[34] In a press release, Apple described iCloud as "a breakthrough set of free new cloud services that work seamlessly with applications on your iPhone, iPad, iPod touch, Mac, or PC to automatically and wirelessly store your content in iCloud and automatically and wirelessly push it to all your devices."[35] The press release went on to explain that "[w]hen anything changes on one of your devices, all of your devices are wirelessly updated almost instantly."[36] The late Steve Jobs, Apple's CEO at the time of iCloud's release, is quoted as saying, "All of this happens automatically and wirelessly, and because it's integrated into our apps you don't even need to think about it—it all just works."[37]

Cloud-computing services are extremely easy to setup and connect to. For example, Apple's website states, "Set up iCloud on all your devices. The rest is automatic."[38] The steps to set up iCloud on a device are as follows: (1) "Make sure your device is running the latest version of [Apple's proprietary operating system] iOS[39]"; (2) "Turn on iCloud"; (3) "Enable automatic downloads"; (4) "Use iCloud on all of your devices."[40] Because all of the applications that run on an iPhone or iPad, including Calendar and Messages, run on iOS, it is virtually impossible to use one of these devices without first setting up an iCloud account.[41]

Google Drive is Google's equivalent to iCloud. Google Drive is a "safe place for all your files" and you can "see your stuff anywhere" as "files in Drive can be reached from any smartphone, tablet, or computer."[42] On Google Drive, a user can access email and store any type of file including photos and videos.[43] Microsoft OneDrive also functions like iCloud and Google Drive.[44] A user can get "files from anywhere, on any device" and can access email while also sharing files and photos.[45]

---

34. *See* Press Release, Apple Inc., Apple Introduces iCloud (June 6, 2011) [hereinafter Apple Press Release], https://www.apple.com/newsroom/2011/06/06Apple-Introduces-iCloud/ [https://perma.cc/7ZQV-QAMH].

35. *Id.* iCloud is not a revolutionary idea but reflects the evolution over time of technological advances to the point where cloud computing is now economically and technically feasible. *See* Gasser, *supra* note 24, at 5. Apple brought the cloud to the average user but cloud systems such as Dropbox existed prior to the introduction of iCloud in 2011. For a discussion of Dropbox, see *infra* note 93.

36. Apple Press Release, *supra* note 34.

37. *Id.*

38. *iCloud Setup*, APPLE INC., http://www.apple.com/icloud/setup/ios.html [https://perma.cc/U2LW-55G9] (last visited Oct. 16, 2017).

39. iOS is the name for the operating system used on Apple iPhones and iPads. *iOS 11*, APPLE INC., https://www.apple.com/ios/ios-11/ [https://perma.cc/S23A-HPXH] (last visited Oct. 16, 2017) (referring to iOS as "[t]he world's most advanced mobile operating system").

40. *iCloud Setup*, *supra* note 38.

41. *iOS 11*, *supra* note 39.

42. GOOGLE DRIVE, https://www.google.com/drive/ [https://perma.cc/ZP8D-QC8C] (last visited Oct. 16, 2017).

43. *Id.*

44. *OneDrive*, MICROSOFT, https://www.onedrive.live.com/about/en-us/ [https://perma.cc/6YXD-4D4S] (last visited Oct. 16, 2017).

45. *Id.*

The purpose of iCloud, Google Drive, and OneDrive is for the user to store all of her data on the cloud, including passwords to applications and email, and sync it with all of her devices for easy access without ever having to think about it once the account has been set up.[46] Part of Apple's website highlights this "seamless experience" and explains that a user can start typing an email or text message on one device and through iCloud, complete the message and respond on another device.[47]

With a better understanding of these cloud-computing systems, it is evident how easy it is for personal information to end up on a variety of devices. After considering the prevalence of situations like the one outlined in the Introduction, one can also see how effortlessly information can end up in the hands of an unintended recipient.

B. How the CFAA Came to Criminalize Computer Usage That "Exceeds Authorized Access"

In 1984, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984[48]—the first federal statute to criminalize unauthorized access to computers.[49] The original statute solely protected classified information, financial records, and credit information stored on computers owned by the government and financial institutions.[50]

Congress then became increasingly concerned with problems of computer fraud and abuse as computers were beginning to become more widespread among businesses, individuals, and the government.[51] Technological advances also created a new type of crime in which individuals used computers to steal, defraud, and abuse the property of others.[52] Courts initially attempted to fit computer crimes into traditional property law, but because much of the property in a computer crime is intangible, there were substantial issues with this approach.[53]

In 1986, Congress ultimately decided the law should be updated to address these types of crimes because existing law could not accommodate abuses of evolving technology.[54] Thus, the Act from 1984 was renamed the Computer Fraud and Abuse Act.[55] In addition to financial crimes, the Senate found that

---

46. *See e.g.*, Apple Press Release, *supra* note 34; *see also supra* note 38 and accompanying text.

47. *iOS 11*, *supra* note 39.

48. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified as amended at 18 U.S.C. § 1030 (2012)).

49. *See* H.R. REP. NO. 98-894, at 6 (1984). There is also a civil right of action in the statute. *See* 18 U.S.C. § 1030(g).

50. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 § 2102(a)(1)–(3).

51. *See* S. REP. NO. 99-432, at 2 (1986).

52. *See id.*

53. *See* H.R. REP. NO. 99-612, at 5 (1986); *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1605–07 (2003).

54. *See* H.R. REP. NO. 99-612, at 5.

55. Computer Fraud and Abuse Act, Pub. L. No. 99-474, § 2, 100 Stat. 1213, 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (2012)).

computer hacking could lead to life-threatening concerns if someone were to gain access to hospital records or government computers.[56] The Senate also determined that "[f]ederal criminal penalties for computer crime are an appropriate punishment for certain acts and can serve to deter would-be computer criminals."[57]

The Senate, intending to enact an antihacking statute, rejected the idea to enact a sweeping federal statute to prevent all computer crimes and instead limited federal jurisdiction to computer crimes where there was a compelling federal interest.[58] This included situations "where computers of the Federal Government or certain financial institutions [were] involved, or where the crime itself [was] interstate in nature."[59]

In 1996, Congress passed another amendment to the CFAA, which expanded the scope of § 1030(a)(2)(C) of the statute.[60] Previously, the CFAA was limited in its protection of unauthorized access,[61] but the 1996 amendment made it a violation of federal law to intentionally access information from any protected computer without authorization or by exceeding authorized access.[62] This part of the statute has not been amended since 1996, thus the text of this provision remains the same.[63] The statute defines "protected computer" as "a computer which is used in or affecting interstate or foreign commerce or communication . . . ."[64] The internet is considered to be an instrumentality and channel of interstate commerce, so every computer connected to the internet is a "protected computer" under the CFAA.[65] In addition, Congress previously determined that "obtain[ing] information" could encompass solely reading the information, which further highlights the expansive reach of the 1996 amendment.[66]

---

56. S. REP. NO. 99-432, at 2–3.

57. *Id.* at 3.

58. *See id.* at 4.

59. *Id.*; *see also infra* note 65 and accompanying text (explaining that the internet is considered to be an instrumentality and channel of interstate commerce).

60. Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201, 110 Stat. 3491, 3491–94.

61. *See supra* note 50 and accompanying text (explaining how § 1030 initially protected only classified information, financial records, and credit information stored on computers owned by the government and financial institutions).

62. *See* Economic Espionage Act § 201.

63. *See* 18 U.S.C. § 1030(a)(2)(C) (2012) ("Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer shall be punished . . . .").

64. 18 U.S.C. § 1030(e)(2)(B).

65. *See* OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 4 (2010); *see also* Kerr, *supra* note 13, at 1568.

66. *See* S. REP. NO. 99-432, at 6 (1986) (noting that "obtaining information" in the statute includes "mere observation of the data"). In 2012, Senator Amy Klobuchar from Minnesota proposed the Cloud Computing Act of 2012. *See* S. 3569, 112th Cong. (2012). This bill attempted to "improve the enforcement of criminal and civil law with respect to cloud computing." *Id.* Although Congress did not pass this bill, it would have given cloud-computing systems more specific and increased protection under the CFAA. Eric Goldman, *The Proposed "Cloud Computing Act of 2012," and How Internet Regulation Can Go Awry*, FORBES (Oct. 2, 2012, 12:01 PM), http://www.forbes.com/sites/ericgoldman/2012/10/02/the-

Although the CFAA was originally enacted to target computer hackers,[67] the statute has been greatly expanded not only by these congressional amendments but also by later interpretation by the courts.[68] As the scope of the CFAA has grown, it has become one of the most widely prosecuted criminal statutes.[69] This is relevant to the hypothetical outlined in the Introduction because, while that situation is not a "hack" in the traditional sense, under the expansive reach of the CFAA, that tablet user could fall within the statute's purview.[70]

Though there are many provisions of the CFAA, § 1030(a)(2)(C)[71] is most applicable to the hypothetical situation previously discussed because it encompasses all "protected computers."[72] Courts commonly interpret all of § 1030(a)(2) in the employment context because employers or the government often use this provision to bring suits against former employees for exceeding authorized computer access in a way that either harms the company or is criminal.[73] Unfortunately, there is little guidance for courts when applying the CFAA outside of the employment context, especially to situations involving the cloud.[74]

According to the statute, the term "exceeds authorized access" from § 1030(a)(2) means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[75] The term "without authorization" from the same section is not defined.

Under the statute, computer intruders can be classified into two categories: "insiders" and "outsiders."[76] The phrase "without authorization" applies to

---

proposed-cloud-computing-act-of-2012-and-how-internet-regulation-can-go-awry/ [https://perma.cc/J8GJ-UZYR].

67. *Merriam-Webster's Dictionary* defines "hacker" as "a person who secretly gets access to a computer system in order to get information, cause damage, etc." *Hacker*, MERRIAM-WEBSTER'S DICTIONARY, http://www.merriam-webster.com/dictionary/hacker [https://perma.cc/C2MU-RRPJ] (last visited Oct. 16, 2017).

68. *See* S. REP. NO. 99-432, at 3–4; *see also* 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, 155–56 (2011); *infra* Part II.

69. Sebastian E. Kaplan, *The Rise of the Computer Fraud and Abuse Case*, FENWICK & WEST LLP (Mar. 20, 2012), https://www.fenwick.com/FenwickDocuments/2012-03-20_Rise_Computer_Fraud_Abuse_Case.pdf [https://perma.cc/J3V8-G3JF] ("Since 2002, complaints alleging a cause of action under the CFAA have increased nearly 600%.").

70. *See infra* Part II.

71. For the text of 18 U.S.C. § 1030(a)(2)(C), see *supra* note 63. Section 1030(a)(2)(A) and (B) are similar provisions that both say "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access," but they apply to information contained in a financial record of a financial institution or information from any department or agency of the United States, respectively, rather than a protected computer. 18 U.S.C. § 1030(a)(2)(A)–(B) (2012).

72. *See supra* note 8 and accompanying text.

73. *See infra* Part II.

74. *See infra* Part II; *see also infra* note 93 (discussing a case that does involve the CFAA as it relates to the cloud but is still in the employment context).

75. 18 U.S.C. § 1030(e)(6).

76. *See* Samantha Jensen, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 90 (2013); Keim, *supra* note 20, at 31–32; Tuma, *supra* note 68, at 175–76.

outside hackers who have no authority to access a computer or server.[77] It is fairly obvious when traditional outside hackers, such as Edward Majerczyk,[78] have accessed a computer "without authorization" because they have no connection to the affected computer and likely breached some type of security to access the information on the computer or server.[79] The phrase "exceeds authorized access" applies to inside hackers who are typically an employee or a friend who has (or had) authorization to access a computer system but abuses that access privilege.[80]

The circuits are split on how authorization under § 1030(a)(2) should be construed as applied to *inside* hackers.[81] The varying views focus on the meaning of the term "exceeds authorized access."[82] This term has led to much discussion in the employment context because employees who are said to have violated the CFAA often have *some* access rights to the employer's computer system as part of their job.[83] A broad interpretation and a narrow interpretation emerged from various circuit court cases.[84] The broad view applies to the misuse of information properly attained while the narrow view is limited to violations of access restrictions and holds that the CFAA does not cover misuse.[85] More specifically, according to the narrow view, "[a]n inside hacker has permission to access limited information on a computer,

77. *See* Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1371–72 (2011).

78. *See supra* notes 1–6 and accompanying text.

79. *See* Urban, *supra* note 77, at 1371–72.

80. *See* Keim, *supra* note 20, at 31 (citing NAT'L CYBERSECURITY & COMMC'NS INTEGRATION CTR., COMBATING THE INSIDER THREAT (2014)). To the extent that Congress was attempting to differentiate between access to the computer itself and the level of permission to obtain information on the computer, these two terms have caused confusion among the courts. *See* Keim, *supra* note 20, at 32. When interpreting the CFAA, the courts have blurred the difference between these two terms even though "without authorization" typically applies to outside hackers and "exceeds authorized access" applies to inside hackers. *See* Tuma, *supra* note 68, at 174. For example, according to the court in *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006), "[t]he difference between 'without authorization' and 'exceeding authorized access' is paper thin, but not quite invisible." *Id.* at 420. The court in *United States v. Drew*, 259 F.R.D 449 (C.D. Cal. 2009), does not differentiate between the two terms. *Id.* at 461. Courts sometimes use the two terms interchangeably when discussing unauthorized access by inside hackers. In the hypothetical from the Introduction, the friend, significant other, or coworker who "exceeds authorized access" when initially requesting to borrow a tablet to browse the internet but actually accesses personal information that is stored on the cloud can be classified as an inside hacker. *See* Keim, *supra* note 20, at 31. For further exploration of this idea, see *infra* Part II.

81. *See infra* Part II.

82. *See infra* Part II; *see also supra* note 80 (explaining how courts do not always distinguish between "without authorization" and "exceeds authorized access" and they are sometimes used interchangeably when referencing inside hackers).

83. *See* Urban, *supra* note 77, at 1372.

84. *See* David J. Schmitt, *The Computer Fraud and Abuse Act Should Not Apply to the Misuse of Information Accessed with Permission*, 47 CREIGHTON L. REV. 423, 424 (2014); *see also infra* Part II. In jurisdictions that follow the narrow interpretation, fewer people are prosecuted under the statute because the CFAA's reach is more limited. Under the broad view, the reach of the CFAA is more expansive and, therefore, more computer users are considered violators of federal law.

85. *See infra* Part II.

but obtains other information on the computer the user did not have permission to access."[86] The broad view, by contrast, "appl[ies] to users who have permission to access computer information, but who 'misuse' the information obtained with permission."[87]

The narrow view is overwhelmingly more popular among scholars, and many articles in this area advocate for courts to adopt the narrow approach[88] or more specifically, to adopt the narrow code-based approach discussed below.[89] The main argument in favor of a version of the narrow approach is that the broad view would overcriminalize computer usage and the narrow approach more accurately aligns with Congress's original intent in enacting this antihacking statute: to deter and punish outside hackers.[90] The U.S. Supreme Court and Congress have yet to resolve this legal dispute and determine the prevailing interpretation of "exceeds authorized access" within the CFAA.[91]

II. THE COMPETING VIEWS OF "EXCEEDS AUTHORIZED ACCESS" BY INSIDERS UNDER THE CFAA AND THEIR APPLICATION TO THE CLOUD

Congress intended for the CFAA to encompass changes in technology, so a court would likely determine that the reach of the CFAA extends to cloud-computing systems, although they were not widely used in the late 1980s when Congress passed the statute.[92] At least one court has interpreted authorization under the CFAA in the employment context as it relates to insiders accessing data on the cloud,[93] but cases involving both the cloud and

86. Schmitt, *supra* note 84, at 432.

87. *Id.* at 432–33.

88. *See generally* Jensen, *supra* note 76; Schmitt, *supra* note 84; Pamela Taylor, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201 (2012); *see also infra* Part II.B (discussing the narrow view).

89. *See generally* Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819 (2009); Kerr, *supra* note 53; Kelsey T. Patterson, *Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489 (2013); *see also infra* Part II.B.3 (explaining the narrow code-based approach).

90. *See generally* Schmitt, *supra* note 84.

91. *See* Tuma, *supra* note 68, at 154. In recent years, Congress has unsuccessfully attempted to resolve the circuit split by proposing an amendment to clarify the meaning of authorization under § 1030. One such amendment, known as Aaron's Law Act of 2015, was introduced in both Houses on April 21, 2015, and proposed striking the definition of "exceeds authorized access" from § 1030(e)(6) and inserting a definition of "access without authorization." H.R. 1918, 114th Cong. (2015); S. 1030, 114th Cong. (2015). The suggested definition of "without authorization" was "to obtain information on a protected computer; that the accesser lacks authorization to obtain; and by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information." H.R. 1918; S. 1030. Congress has not passed this bill.

92. *See* S. REP. NO. 104-357, at 5 (1996); *see also supra* notes 15–17 and accompanying text.

93. *See* Frisco Med. Ctr., L.L.P. v. Bledsoe, 147 F. Supp. 3d 646, 652 (E.D. Tex. 2015). In this case, the defendants were hospital employees who exceeded their authorization and violated § 1030(a)(2)(C) of the CFAA when they used Dropbox to upload confidential files

the CFAA are limited. Instead, the main views to defining authorization have emerged from case law specific to discussions of insiders accessing a computer in the employment context without mention of the cloud.

Within the narrow and broad interpretations of authorization under the CFAA, courts use varying approaches to explain the definition of "exceeds authorized access" as applied to inside hackers.[94] These approaches are classified as (1) the broad agency view, (2) the broad contract-based view, (3) the narrow contract-based view, and (4) the narrow code-based view. Part II.A discusses the broad approaches to interpreting the CFAA while Part II.B analyzes the narrow approaches. Both Parts apply these interpretations to the hypothetical from the Introduction to show how they would operate in a context outside of the employer-employee relationship.[95]

A. The Broad View: Misuse of Information Properly Obtained Is Sufficient for Insiders to "Exceed[] Authorized Access"

When applying the broad view of the CFAA, courts in the First, Fifth, Seventh, and Eleventh Circuits have explored the misuse of information properly obtained—the broad standard[96] for determining when an insider "exceeds authorized access"—using different lenses.[97] These two lenses are the broad agency approach and the broad contract-based approach. Part II.A.1 analyzes the broad agency approach and Part II.A.2 applies the broad agency approach to this Note's cloud-computing hypothetical. Then, Part II.A.3 discusses the broad contract-based approach and Part II.A.4 applies the broad contract-based approach to the same hypothetical.

1. The Broad View of the CFAA Under the Agency Approach

The agency approach to interpreting the CFAA is grounded in agency law.[98] The court in *Shurgard Storage Centers, Inc., v. Safeguard Self*

from the hospital system to their home computer. *Id.* at 646, 652, 659. Dropbox is an internet service that "uses 'cloud' storage to enable users to store and share files with others across the Internet using file synchronization. When files are uploaded to Dropbox by a user, they automatically 'sync' with another computer selected by the user, meaning that the files are transferred from one computer to another." *Id.* at 652. Dropbox is another cloud-computing system that functions like iCloud, Google Drive, and OneDrive. *See* DROPBOX, https://www.dropbox.com [https://perma.cc/L4TY-AKXN] (last visited Oct. 16, 2017); *see also supra* Part I.A (explaining the function and purpose of the cloud).

94. *See supra* note 80 (explaining how the courts have blurred the difference between "without authorization" and "exceeds authorized access" and often use the terms interchangeably). This Note's focus is on the CFAA as a criminal statute. Though some of the cases discussed in Part II are brought in the civil context, there is no difference in how the interpretations of "exceeds authorized access" are applied to criminal versus civil cases.

95. *See supra* note 8 and accompanying text.

96. *See supra* text accompanying note 85.

97. *See generally* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

98. *See* Field, *supra* note 89, at 823; Jensen, *supra* note 76, at 103.

Storage, Inc.[99] was the first to apply agency theory to interpret the CFAA.[100] The plaintiff Shurgard Storage Centers and the defendant Safeguard Self Storage were competitors in the self-storage business.[101] The defendant offered Eric Leland, a manager of the plaintiff, a position with its company.[102] While still an employee of Shurgard but acting as an agent for Safeguard, Leland used his position at Shurgard to access confidential information, which he then emailed to Safeguard.[103] Shurgard alleged that Safeguard violated § 1030(a)(2)(C) of the CFAA.[104] When making its decision, the court relied upon section 112 of the Restatement (Second) of Agency which states that, "[u]nless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[105] The court explained that "when Mr. Leland or other former employees used the plaintiff's computers and information on those computers in an improper way they were 'without authorization.'"[106] Though the court did not find it necessary to subsequently determine whether Leland had also "exceed[ed] authorized access" under the CFAA, courts often do not differentiate between "exceeds authorized access" and "without authorization" when interpreting the statute.[107]

The Seventh Circuit similarly adopted the broad agency approach in *International Airport Centers, L.L.C. v. Citrin*.[108] International Airport Centers (IAC) employed Citrin to identify properties that IAC might want to acquire and IAC lent Citrin a laptop to use in the course of his employment.[109] When Citrin decided to leave his position at IAC, he deleted the data on the laptop using a secure erasure program before returning it.[110] IAC alleged that Citrin violated § 1030(a)(5)(A)(i) of the CFAA when he erased the laptop.[111]

---

99. 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

100. *See* Jensen, *supra* note 76, at 104.

101. *Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1122.

102. *Id.* at 1123.

103. *Id.*

104. *See id.*; *see also* 18 U.S.C. § 1030(a)(2)(C) (2012).

105. RESTATEMENT (SECOND) OF AGENCY § 112 (AM. LAW INST. 1958); *see also Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1124–25.

106. *Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1124.

107. *See id.* at 1125 n.4; *see also supra* note 80 (explaining how courts have blurred the difference between "without authorization" and "exceeds authorized access").

108. 440 F.3d 418 (7th Cir. 2006).

109. *Id.* at 419.

110. *Id.*

111. *See id.* The section of the CFAA quoted in this opinion has since been amended and is now § 1030(a)(5)(A). This provision states, "Whoever 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; shall be punished as provided in subsection (c) of this section." 18 U.S.C. § 1030(a)(5)(A) (2012). Despite this section's inapplicability to the hypothetical introduced earlier in this Note, the reasoning that the Seventh Circuit applies is still applicable to the other sections of the statute, including § 1030(a)(2)(C).

The court, in an opinion written by Judge Richard A. Posner, relied on agency law to determine that Citrin violated the CFAA by misusing information properly obtained.[112] The court explained, "Citrin's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship."[113] Like the court in *Shurgard*, the court here referenced section 112 of the Restatement (Second) of Agency,[114] but also relied on another section in making this determination.[115]

Although Citrin was still an employee when he accessed and deleted the files, he terminated his agency relationship with IAC when he elected to quit and therefore he no longer had access to use the laptop.[116] Under this approach, a breach of the duty of loyalty leads to a violation of the CFAA regardless of the employer's ignorance of any breach.[117] The Seventh Circuit concluded that an employee acts "without authorization" or "exceeds authorized access" when his interests are no longer aligned with the employer's.[118] The court adopted the broad approach to the CFAA by focusing on computer misuse by the employee, rather than an access restriction put in place by the employer, in determining that Citrin violated the CFAA.[119]

2. The Broad Agency View Applied to the Cloud

Under the broad agency view of authorization, as interpreted by the courts in the employment setting, an employee "exceeds authorized access" when she acquires interests that are adverse to the employer or breaches the duty of loyalty by misusing information that was otherwise properly obtained.[120] Although the same rules of agency theory do not apply in the hypothetical from the Introduction because the hypothetical is not based in the employment context, the reasoning is still applicable. An individual who accesses another's cloud account and obtains personal information still acquires interests adverse to the owner of the device and could misuse the information, thus "exceed[ing] authorized access" in the same way.[121] Consequently, when applying the broad agency approach of authorization outside of the employment context to a scenario involving cloud computing,

112. *See Int'l Airport Ctrs.*, 440 F.3d at 420–21.
113. *Id.*
114. *See supra* notes 105–06 and accompanying text.
115. *See Int'l Airport Ctrs.*, 440 F.3d at 420; *see also* RESTATEMENT (SECOND) OF AGENCY § 387 (AM. LAW INST. 1958) ("Unless otherwise agreed, an agent is subject to a duty to his principal to act solely for the benefit of the principal in all matters connected with his agency.").
116. *See Int'l Airport Ctrs.*, 440 F.3d at 419–21.
117. *See id.* at 421.
118. *Id.* at 420–21.
119. *See id.*; *see also* Patterson, *supra* note 89, at 502.
120. *See Int'l Airport Ctrs.*, 440 F.3d at 420–21; *see also supra* Part II.A.1.
121. *See Int'l Airport Ctrs.*, 440 F.3d at 420–21; *see also* Shurgard Storage Ctrs., Inc., v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000).

an individual in this Note's hypothetical situation could also be found to violate the CFAA.

3. The Broad View of the CFAA Under the Contract-Based Approach

In the employment setting, some courts apply contract principles to the misuse of computer information. Using this interpretation, an individual may be liable under the CFAA when she violates an implicit or explicit contract between the two parties that outlines the employee's authorization to use a computer.[122] In *EF Cultural Travel BV v. Explorica, Inc.*,[123] Philip Gormley, an Explorica employee, signed a confidentiality agreement when previously employed by Explorica's competitor, EF, which prohibited him from disclosing any of EF's confidential information to any third party.[124] In his new position at Explorica, Gormley used proprietary information from his experience at EF to assist in creating a program for Explorica to record large amounts of information from EF's website, which was used to undercut EF's prices.[125] EF sued Explorica alleging that the use of this software program violated the CFAA.[126]

The First Circuit analyzed the CFAA definition of "exceeds authorized access" and determined that Explorica's *use* of EF's travel codes was beyond the usual authorized purpose of EF's website.[127] In addition, Gormley breached his confidentiality agreement by misusing information to assist in creating the program, thereby exceeding his authorization in using EF's website.[128] In short, the First Circuit applied the broad contract-based interpretation of the CFAA and decided that Explorica and Gormley "exceed[ed] authorized access" by engaging in computer misuse and that the contract that existed between the parties limited Explorica's authorization.[129]

The Fifth Circuit also adopted the broad contract-based view of the CFAA in its opinion in *United States v. John*,[130] when it held that an employee could violate the CFAA by "exceed[ing] authorized access" under an employer's computer-use policy.[131] The court reasoned that authorization includes limits placed on the use of information properly obtained "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 [is] in furtherance of or to perpetrate a crime."[132]

The defendant, Eva-Lavon John, obtained customer information that she was authorized to access and misused that information by providing it to her

122. *See* Field, *supra* note 89, at 827.
123. 274 F.3d 577 (1st Cir. 2001).
124. *Id.* at 582.
125. *Id.* at 582–83.
126. *Id.* at 577–78.
127. *Id.* at 583.
128. *Id.*
129. *See generally id.*
130. 597 F.3d 263 (5th Cir. 2010).
131. *See id.* at 272.
132. *Id.* at 271.

half brother who then used the information to engage in fraud.[133] She was convicted of a criminal violation of the CFAA for "exceed[ing] authorized access" to a protected computer under § 1030(a)(2)(A) and (C).[134] The court held that John's use of this information violated employee policies because her access to the computer systems was limited in that she could only access the customer information for business reasons.[135] The Fifth Circuit agreed with the First Circuit's reasoning in *EF Cultural Travel BV*[136] and held that an employee could "exceed[] authorized access" and violate the CFAA by exceeding the purpose for which access was initially given.[137]

In addition to the First and Fifth Circuits, the Eleventh Circuit in *United States v. Rodriguez*[138] also followed the broad contract-based approach to interpreting authorization under the CFAA. The court held that the defendant, Roberto Rodriguez, violated § 1030(a)(2)(B)[139] when he accessed personal information in the Social Security Administration database for nonbusiness reasons.[140] The court reasoned that Rodriguez's use of the database violated the administration's policy.[141] Thus, it was irrelevant that Rodriguez only accessed information that he was authorized to obtain.[142] Accordingly, the Eleventh Circuit held Rodriguez exceeded his access to the computer system when he misused information, consequently violating the CFAA.[143]

4. The Broad Contract-Based View Applied to the Cloud

Under the broad contract-based view of the CFAA in the employment context, an employee is found to violate the statute by misusing information and breaching an implicit or explicit contract outlining authorization for computer usage.[144] The explicit contract between the parties can be a

133. *Id.* at 269.

134. *Id.* at 269–70. Section 1030(a)(2)(A) says, "Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer[,] . . . or contained in a file of a consumer reporting agency on a consumer . . . shall be punished . . . ." 18 U.S.C. § 1030(a)(2)(A) (2012). Although § 1030(a)(2)(A) is not the focus of this Note, the reasoning of the court in this case is still applicable because John also violated § 1030(a)(2)(C), and both sections involve "exceed[ing] authorized access." *See also supra* note 71.

135. *John*, 597 F.3d at 271–72.

136. For a discussion of this case, see *supra* notes 123–29 and accompanying text.

137. *See John*, 597 F.3d at 272.

138. 628 F.3d 1258 (11th Cir. 2010).

139. Section 1030(a)(2)(B) says, "Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any department or agency of the United States shall be punished . . . ." 18 U.S.C. § 1030(a)(2)(B). Though this section of the CFAA is not applicable to the hypothetical proposed in the Introduction, the court's reasoning in *Rodriguez* applies because § 1030(a)(2)(B) still involves "exceed[ing] authorized access." *See supra* note 71.

140. *Rodriguez*, 628 F.3d at 1263.

141. *Id.*

142. *Id.*

143. *Id.*

144. *See supra* note 122 and accompanying text (discussing implicit and explicit contracts); *see also supra* Part II.A.3.

confidentiality agreement,[145] computer-use policy,[146] or employment policy.[147]

Although this Note's hypothetical contains no explicit written contract or policy and takes place outside the employment context, this interpretation of CFAA violations also encompasses implicit contracts.[148] The hypothetical arguably involves an implicit oral contract because it can be implied that the tablet was lent out after a verbal agreement that it would be used for internet browsing purposes only. According to *Black's Law Dictionary*, an oral or parol contract is "a contract . . . that is not in writing or is only partially in writing."[149] The law recognizes oral contracts although written contracts are usually preferred.[150]

If the tablet user from the hypothetical scenario misuses her authorized access to the internet to instead view something like the device owner's Google Drive account, which is on the cloud and accessible through the internet browser, she arguably breaches the oral contract between the two parties.[151] These actions could be considered a misuse of information and a violation of the CFAA because although the tablet user was allowed to access the internet browser, that access was limited.[152] The user arguably "exceed[ed] authorized access" because she exceeded the purpose for which authorization was given when she viewed cloud data available through the browser.[153]

B. The Narrow View: Violations of Access Restrictions Is Sufficient for Insiders to "Exceed[] Authorized Access"

Courts in the Second, Fourth, and Ninth Circuits follow the narrow view—rather than the broad view—of interpreting authorization for insiders for purposes of the CFAA.[154] Under this more limited view, an individual violates the CFAA when she has permission to access information on a computer but instead obtains other information on the computer that she lacked permission to access.[155] In these jurisdictions, unlike in jurisdictions that follow the broad view, the CFAA is not applicable when an individual

145. *See supra* note 129 and accompanying text. *See generally* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

146. *See supra* notes 130–32 and accompanying text. *See generally* United States v. John, 597 F.3d 263 (5th Cir. 2010).

147. *See supra* note 142 and accompanying text. *See generally Rodriguez*, 628 F.3d 1258.

148. *See supra* note 122 and accompanying text.

149. *Contract*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining parol contract). Another name for parol contract is "oral contract." *Id.*

150. *See* Fenix Enters., Inc. v. M & M Mortg. Corp., 624 F. Supp. 2d 834, 841–42 (S.D. Ohio 2009).

151. *See supra* Parts I.A, II.A.3.

152. *See, e.g.*, United States v. John, 597 F.3d 263, 271–72 (5th Cir. 2010).

153. *See id.*

154. *See generally* United States v. Valle, 807 F.3d 508 (2d Cir. 2015); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

155. *See supra* note 86 and accompanying text.

misuses information that was properly obtained.[156] When applying the narrow view, courts analyze violations of access restrictions by insiders using two different approaches: the narrow contract-based approach and the narrow code-based approach. Accordingly, Part II.B.1 explores the narrow contract-based approach and Part II.B.2 applies the narrow contract-based approach to this Note's cloud-computing scenario. Then, Part II.B.3 discusses the narrow code-based approach and Part II.B.4 applies the narrow code-based approach to the same scenario.

1. The Narrow View of the CFAA Under the Contract-Based Approach

The narrow contract-based approach holds that there is no violation of the CFAA when an employer's policy restricts an employee's *use* of information rather than *access to* the information.[157] Instead, under this approach, the CFAA is applicable only when an employee exceeds the employer's authorized access.[158]

The Ninth Circuit applied this narrow approach to authorization in *United States v. Nosal*.[159] In this case, David Nosal, a former Korn/Ferry employee who left the company to start his own business, convinced some of his former coworkers to use their login credentials to download confidential information from Korn/Ferry and send it to Nosal.[160] Korn/Ferry employees could access the database but there was a policy that restricted them from disclosing confidential information.[161] Nosal was charged with violating § 1030(a)(4)[162] of the CFAA for aiding and abetting his former coworkers in exceeding their authorized access to the Korn/Ferry computers.[163] The court reasoned that although Nosal's accomplices misused the information they were authorized to access, Nosal had not violated the statute because the term "'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*."[164]

156. *See* Schmitt, *supra* note 84, at 439; *see also supra* Part II.A.

157. *See* Schmitt, *supra* note 84, at 432–33.

158. *See generally Valle*, 807 F.3d 508; *WEC Carolina Energy Sols.*, 687 F.3d 199; *Nosal*, 676 F.3d 854.

159. 676 F.3d 854 (9th Cir. 2012).

160. *Id.* at 856.

161. *Id.*

162. Section 1030(a)(4) provides:

> Whoever knowingly 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 shall be punished . . . ."

18 U.S.C. § 1030(a)(4) (2012). It is not likely that an individual who obtains access to another individual's cloud-computing system would violate this section of the CFAA but the reasoning that the court applies is still applicable to the other sections of the statute including § 1030(a)(2)(C).

163. *Nosal*, 676 F.3d at 856; *see also* 18 U.S.C. § 1030(a)(4).

164. *Nosal*, 676 F.3d at 863–64.

Therefore, the government's charges failed to meet the elements of "without authorization" or "exceeds authorized access" under the statute.[165]

The Ninth Circuit explained that if the CFAA applied broadly to use restrictions and violations of the duty of loyalty rather than access restrictions,[166] then the CFAA would become too expansive.[167] For example, using a work computer for personal use is commonly prohibited by employer computer-use policies.[168] According to the court in *Nosal*, if it adopted the broad view, employees who used personal email at work or checked sports scores on ESPN could be subject to criminal liability under the CFAA.[169] The court reasoned that "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose."[170]

Like the Ninth Circuit, the Fourth Circuit in *WEC Carolina Energy Solutions LLC v. Miller*[171] also adopted the narrow contract-based approach. There, defendant Mike Miller resigned as an employee for WEC and later made a presentation to a potential WEC customer as a representative for his new employer, Arc Energy Service, Inc., a competitor of WEC.[172] After the customer chose to work with Arc over WEC, WEC alleged that when Miller was still an employee, he downloaded confidential information from WEC's system, emailed this information to his personal email address, and used it to win over the potential customer.[173] Miller was privy to this information as part of his employment, but WEC had a policy that prohibited using confidential information without authorization or downloading the information to a personal computer.[174] WEC sued Miller claiming he violated multiple provisions of the CFAA including § 1030(a)(2)(C).[175]

The court concluded that "an employee 'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access."[176] The court also noted that this interpretation does not extend to the misuse of information properly obtained.[177] The Fourth Circuit agreed with the Ninth Circuit's opinion in *Nosal* and determined that when an employee has access

165. *Id.* at 864.
166. *Id.* at 862–63; *supra* Part II.A.
167. *See Nosal*, 676 F.3d at 857.
168. *See id.* at 860.
169. *Id.*
170. *Id.* at 857. Courts and scholars have expressed concern about overcriminalization of the CFAA because if authorization is interpreted too broadly, many everyday computer activities could become violations of the CFAA. *See id.* at 860; *see also* Patterson, *supra* note 89, at 513; *supra* notes 88–90 and accompanying text. This is one of the main arguments against the broad view of interpreting authorization.
171. 687 F.3d 199 (4th Cir. 2012).
172. *Id.* at 201.
173. *Id.* at 202.
174. *Id.*
175. *Id.* at 203. WEC alleged that Miller also violated § 1030(a)(4), (a)(5)(B), and (a)(5)(C). *Id.*
176. *Id.* at 204.
177. *Id.*

to information and then misuses the information, his "manner" of access remains valid.[178] Thus, Miller was not liable under the CFAA for the improper use of information accessed with authorization.[179] The court also rejected the broad agency and broad contract approaches for reasons that are similar to those relied on by the Ninth Circuit in *Nosal*.[180]

Most recently, in *United States v. Valle*,[181] the Second Circuit followed the Ninth and Fourth Circuits and adopted the narrow contract-based approach.[182] The Second Circuit determined that Valle did not "exceed[] authorized access" when he used his authorization to a computer program, which allows police officers to search secure databases, for a purpose unrelated to his employment.[183] The court reasoned that although Valle violated the terms of his employment, he did not violate the CFAA because he only used his computer access to obtain information that he was authorized to view; thus, his misuse of this information for personal reasons was irrelevant.[184]

2. The Narrow Contract-Based View Applied to the Cloud

Under the narrow contract-based view of authorization in the employment context, an employee "exceeds authorized access" when she has approval, through a contract such as an employment policy, to access a computer but goes beyond the scope of that approval to access additional information.[185] This approach does not apply to the misuse of information properly obtained.[186]

Although there is no written contract in this Note's hypothetical involving the cloud, there likely was a parol or oral contract between the two parties that usage of the tablet would be for internet browsing only.[187] Therefore, accessing personal information like messages, emails, or pictures that are on the device because they are stored in the cloud, would qualify as "exceed[ing] authorized access."[188] This would be a violation of the CFAA under the narrow contract-based approach because the tablet user went beyond the

178. *See id.* at 205; *supra* notes 159–70 and accompanying text (discussing the Ninth Circuit's decision in United States v. Nosal, 676 F.3d 854 (9th Cir. 2012)).

179. *See WEC Carolina Energy Sols. LLC*, 687 F.3d at 205.

180. *See id.* at 206; *supra* notes 167–70 and accompanying text (noting the *Nosal* court's explanation of the possible far-reaching effects of the broad interpretation of authorization under the CFAA and that this interpretation was not intended by Congress).

181. 807 F.3d 508 (2d Cir. 2015).

182. *See id.* at 527; *see also* Michael L. Levy, *A Proposed Amendment to 18 U.S.C. § 1030—The Problem of Employee Theft*, 84 GEO. WASH. L. REV. 1591, 1600–01 (2016).

183. *Valle*, 807 F.3d at 523.

184. *See id.* at 523–24.

185. *See, e.g.*, United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012).

186. *See* WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012); *supra* note 177 and accompanying text.

187. *See supra* notes 149–50 and accompanying text (defining parol contracts).

188. *See supra* Part II.B.1.

scope of her authorization when she accessed information outside of the internet browser that she was not permitted to access.[189]

The Northern District of California faced a factually analogous situation to this Note's hypothetical scenario in *Weingand v. Harland Financial Solutions, Inc.*,[190] and came to a similar conclusion, though the cloud was not a factor. There, Harland brought CFAA charges against its former employee, Weingand, arguing that after termination, Weingand received permission to access Harland's computer system to retrieve his "personal files" but that he did not have authorization to access the additional business files that he copied.[191] The court determined that there was "a reasonable inference that [Weingand's] authorization extended only to accessing and copying said 'personal files' and that he exceeded that authorization" when he accessed company files.[192] Thus, Harland had a valid claim against Weingand under the CFAA.[193] This result may help to understand the hypothetical scenario discussed above in which a user, who entered into an implied contract with a friend to use her device for the limited purpose of internet browsing, may be held liable under the CFAA for exceeding that authorization.

3. The Narrow View of the CFAA Under the Code-Based Approach

The narrow code-based view of authorization under the CFAA is the narrowest approach, which was first proposed by scholar Orin Kerr and has been advocated for by other academics.[194] Unlike the agency approach and the contract-based approach, this interpretation requires a user to bypass security measures intended to restrict access to a computer to trigger a violation of the CFAA.[195] According to Professor Kerr, users can circumvent a code either by "engag[ing] in false identification" by using someone else's password or by "exploit[ing] a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges."[196]

Although no circuit courts have explicitly adopted the narrow code-based approach, this approach is still one of the leading interpretations of the CFAA among academics[197] and is referred to as the plain-meaning theory in some

189. *See, e.g.*, *Nosal*, 676 F.3d at 860–61.
190. No. C-11-3109 EMC, 2012 WL 2327660 (N.D. Cal. June 19, 2012).
191. *See id.* at *1–2.
192. *Id.* at *2. The court relied on the Ninth Circuit's reasoning in *Nosal*. *See supra* notes 159–70 and accompanying text.
193. *See Weingand*, 2012 WL 2327660, at *2.
194. *See generally* Kerr, *supra* note 53; Patterson, *supra* note 89.
195. *See* Kerr, *supra* note 53, at 1644–45.
196. *Id.*
197. *See* Andrew T. Hernacki, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1561 (2012); *see also* Patterson, *supra* note 89, at 506–10. One scholar has noted that a 9th Circuit case is the "only recent circuit court opinion that seems to have implemented anything close to the code-based theory in the employment context." Patterson, *supra* note 89, at 506–10; *see also* LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

district court opinions.[198] The courts that reach results consistent with the code-based approach look to the plain language of the CFAA to determine whether an individual has "exceed[ed] authorized access" rather than looking to outside sources such as the Restatement (Second) of Agency or contract theory.[199] For instance, in *Black & Decker (US), Inc. v. Smith*,[200] the court reviewed the text of the statute itself and determined that it would only look to other authorities if the language was ambiguous.[201] The court also focused on the statute's legislative history and was persuaded by Congress's intent for enacting the CFAA.[202] Because the CFAA is a criminal statute, under this view, courts apply the rule of lenity, which requires that ambiguities in a criminal statute be resolved in favor of the defendant.[203] In *Remedpar, Inc. v. Allparts Medical, LLC*,[204] the court analyzed the holding of *Black & Decker* and made a similar determination about the meaning of authorization under the CFAA.[205]

4. The Narrow Code-Based View Applied to the Cloud

Under this final approach to interpreting authorization under the CFAA, a user violates the statute by engaging in "false identification" and circumventing a security measure intended to restrict access, such as a password.[206] Cloud-computing systems are capable of storing the passwords for email or other applications so the account can be easily accessed in the future.[207] Although the user in this Note's hypothetical has permission to use the tablet and may have the passcode to unlock the device, she could arguably still "exceed[] authorized access" by opening any of the accounts accessible because the password is saved on the cloud.[208] Because the tablet user's authorization only extends to internet browsing, these actions could be considered "false identification" and a violation of the CFAA under this approach.[209]

198. *See, e.g.*, Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 618 (E.D. Pa. 2013); JBCHoldings NY, LLC. v. Pakter, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013); Remedpar, Inc. v. Allparts Med., LLC, 683 F. Supp. 2d 605, 616 (M.D. Tenn. 2010); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 935 (W.D. Tenn. 2008); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *4–5 (M.D. Fla. Aug. 1, 2006).

199. *See supra* note 198; *see also* Urban *supra* note 77, at 1380 n.66.

200. 568 F. Supp. 2d 929 (W.D. Tenn. 2008).

201. *See id.* at 934–35.

202. *See id.*; *see also supra* Part I.B (discussing how Congress intended for the CFAA to be an antihacking statute).

203. *Black & Decker*, 568 F. Supp. 2d at 934–35.

204. 683 F. Supp. 2d 605 (M.D. Tenn. 2010).

205. *See id.* at 610–13.

206. *See* Kerr, *supra* note 53, at 1644; *supra* note 195 and accompanying text.

207. *See supra* Part I.A.

208. *See supra* Part II.B.3.

209. *See* Kerr, *supra* note 53, at 1644–45.

III. AMENDING THE CFAA TO ADDRESS THE CLOUD WHEN NONE OF THE CURRENT INTERPRETATIONS OF "EXCEEDS AUTHORIZED ACCESS" SUFFICE

Despite the circuit courts' adoption of multiple different interpretations of what it means for insiders to "exceed[] authorized access,"[210] the CFAA remains the dominant statute for addressing computer-based crimes and is relevant in most cases involving access to information on a computer.[211] The statute was intended to incorporate technological advances that emerge over time—indeed, the CFAA as it is currently written can, in theory, encompass new advances that were not yet invented when the statute was drafted, such as the cloud.[212] The cloud's capabilities greatly expand the reach of the term "protected computer," which leads to the possibility of increased violations of the CFAA under all four approaches of interpretation by insiders.[213] Many of these potential violations should not be considered criminal under federal law, and the statute's original drafters did not intend for them to be classified as such.[214]

This Part argues that all four approaches to interpreting authorization under the CFAA are too broad when applied to cloud computing, resulting in the characterization of harmless computer users as hackers, and suggests an amendment to the statute to resolve this unjust result. Part III.A proposes that, although the framework for interpreting the CFAA is applicable to situations involving authorization to access data on the cloud, all of the current interpretations to define authorization are overinclusive when applied to cloud computing. Part III.B then advocates for an amendment to the CFAA to address access to the cloud specifically and to limit the reach of the CFAA in this area.

A. All Approaches to Interpreting "Exceeds Authorized Access" Produce an Inequitable Result When Applied to the Cloud

Though cases involving cloud computing and the CFAA have started to make their way into the courts,[215] the CFAA is commonly interpreted in the employment context.[216] The circuit courts are split between different interpretations of what it means for insiders to "exceed[] authorized access" under the statute.[217]

---

210. *See supra* Part II.

211. *See supra* note 20. This Note discusses a novel issue because while access to the cloud has been analyzed in terms of the Fourth Amendment, the scholarship applying the CFAA to the cloud is extremely limited despite the statute's importance to prosecuting computer crimes and the cloud's increasing prevalence. *See* text accompanying *supra* note 11.

212. *See supra* notes 15–17 and accompanying text.

213. *See supra* Part I.A.

214. *See supra* Part I.B.

215. *See supra* note 93 and accompanying text (discussing *Frisco Medical Center, L.L.P. v. Bledsoe*, 147 F. Supp. 3d 646 (E.D. Texas 2015), a case involving Dropbox and the CFAA).

216. *See supra* Part II.

217. *See supra* Part II.

Many scholars advocate for the narrow interpretation to dominate.[218] There are an abundance of articles arguing for jurisdictions to adopt the narrow view generally or the narrow code-based view specifically.[219] The predominant argument is that the broad view to interpreting the CFAA overcriminalizes actions taken by the average computer user and that some variation of the narrow view is the only way to read the statute adequately.[220] The problem with these arguments is that all four approaches to interpreting "exceeds authorized access" are too broad when applied to accessing data on the cloud and can support a finding that an innocuous computer user violated federal law.[221] As such, the CFAA cannot adequately handle this new type of technology.[222] The current interpretations of authorization would even unjustly classify this Note's hypothetical tablet user as a violator of the CFAA.[223]

Although the narrow view is likely the better way to interpret authorization under the CFAA, even this approach leads to overcriminalization of computer usage when applied to the cloud.[224] Consequently, resolving the circuit split is unnecessary for the purpose of this Note, as none of the circuits have adopted an interpretation of authorization that is suitable when applied to accessing data on the cloud.[225]

Some may believe that the current interpretations of authorization are fair because they punish anyone (whether an insider or an outsider) who exceeds authorization to a computer, but this view is not in line with the legislative history of the statute.[226] The CFAA was initially enacted by Congress as an antihacking statute[227] to provide a statutory means of prosecuting outsiders who actively tried to steal information, such as Edward Majerczyk,[228] not a friend or coworker who viewed personal information on someone else's tablet.[229] Hence, it is inequitable to find that the average computer user has violated the CFAA when accessing information that is easily obtainable through the cloud when using a device.[230] Unfortunately, the expansive amendments passed by Congress over the past thirty years and the varying interpretations of what it means to "exceed[] authorized access" under the CFAA that have emerged from the courts have led to this result.[231]

---

218. *See supra* notes 88–89 and accompanying text.
219. *See supra* notes 88–89 and accompanying text.
220. *See supra* text accompanying note 90. For a discussion of the Ninth Circuit's opinion advocating for the narrow view, see *supra* notes 166–70 and accompanying text.
221. *See supra* Parts II.A.2, II.A.4, II.B.2, II.B.4.
222. *See supra* Part II.
223. *See supra* Part II.
224. *See supra* Part II.
225. *See supra* Part II.
226. *See supra* Part I.B.
227. *See supra* Part I.B (explaining the purpose of the CFAA).
228. *See supra* notes 1–6 and accompanying text.
229. *See supra* Part I.B (discussing the purpose of the CFAA).
230. *See supra* Part I.A.
231. *See supra* Parts I.B, II.

As usage of the cloud becomes more widespread, it is important to clarify and amend the CFAA with respect to cloud computing.[232] It is only a matter of time before a prosecutor somewhere decides to make an example out of a computer user who harmlessly accesses another person's cloud account, like the individual in this Note's hypothetical.[233] Cloud-computing systems are unique in that anything on the cloud syncs to all devices connected to that cloud account and thus, the cloud deserves special treatment under the CFAA.[234] Therefore, it is up to Congress to change the law.

B. A New CFAA Amendment: One That Acknowledges the Cloud and Criminalizes Actions by Outsiders

Since the statute's enactment in the 1980s, multiple amendments have expanded the reach of the CFAA but none have specifically mentioned the cloud or determined how cloud computing fits into the framework of the law.[235] In 2012, the Senate attempted to address cloud computing within the CFAA by proposing the Cloud Computing Act of 2012, but this bill was not ultimately adopted into law.[236] Thus, under the current text of the Act, the cloud is not mentioned.[237] The best solution to resolve the inequity that results from the treatment of cloud computing under the CFAA is for Congress to amend the statute to specifically address the cloud. This is the only result that adequately protects innocuous insiders and advises courts, including the Supreme Court, on how to treat access to data on the cloud under federal law.[238]

Congress should create a new provision of the CFAA modeled after § 1030(a)(2)(C)[239] that specifically addresses cloud computing and is grounded in the true purpose of the CFAA—criminalizing the actions of outsiders.[240] The new provision should read: "Whoever intentionally accesses data on the cloud *without authorization* and thereby obtains information from any protected computer shall be punished." In situations where the violation of the CFAA is suspected to involve the cloud, this new provision would apply, but it would not replace the current § 1030(a)(2)(C), which would still apply to situations in the employment context or other instances that may occur outside of the cloud.[241]

---

232. *See supra* note 11 (discussing how these types of cases are likely to become more common as people increasingly use the cloud).

233. For a discussion of the importance of this issue, see *supra* note 11.

234. *See supra* Part I.A.

235. *See supra* Part I.B.

236. For a discussion on the Cloud Computing Act of 2012, *see supra* note 66.

237. *See* 18 U.S.C. § 1030 (2012).

238. *See supra* note 11 and accompanying text (discussing how this issue involving the cloud is likely to become more prevalent in the future as usage of cloud computing expands).

239. *See supra* note 63 and accompanying text.

240. *See supra* Part I.B.

241. The resolution of the circuit split and whether the current provisions of the CFAA should be amended is outside the scope of this Note. *See supra* note 225 and accompanying text.

In addition, Congress should include a definition of "without authorization" as part of the amendment, like the one that was proposed by Congress in a 2015 bill, to ensure that courts in all jurisdictions apply the CFAA consistently.[242] The definition of "without authorization" must specify that the provision of the statute only applies to outsiders or hackers who: (1) have no authority to access a computer or cloud account; (2) have no connection to the affected computer or cloud account; and (3) likely broke through some type of security to gain access to information on the computer or the cloud.[243] Finally, this amendment should also include the standard definition of "cloud computing" commonly cited by scholars and established by the NIST to clarify what is meant by cloud computing and what is covered under this new provision.[244]

The difference between this proposed amendment to the CFAA and the current provision in § 1030(a)(2)(C) is that, for cases where the cloud is a factor, an individual only violates the Act when she acts without any type of authorization and is considered an outsider rather than an insider.[245] The part of the statute that involves "exceed[ing] authorized access" and applies to insiders is omitted because that phrase in the current statute could lead to the overcriminalization of computer users in situations involving the cloud.[246] This is an essential amendment because it would only classify outside hackers, who have no authorization to access cloud data in the first place, as violators of the CFAA, which was the original intent of the statute.[247] As evidenced throughout this Note, no matter which interpretation of authorization a court applies, situations involving the cloud could be a violation of the CFAA under all of them, even when the action taken on a computer is outside the scope of the statute's true purpose.[248] This result can and should be remedied by congressional action.

CONCLUSION

The framework established to interpret authorization under the Computer Fraud and Abuse Act in the employment context can be applied—and, in fact, by its design does apply—to interpreting authorization outside the employment context in situations involving cloud-computing systems. But while cloud-computing hacks by outsiders fall within the mischief the statute was designed to combat, the current interpretations of the Act render it too expansive and would result in the characterization of many innocuous insiders as computer hackers under federal law. In essence, the CFAA is ill-

242. For a discussion of the proposed 2015 amendment to the CFAA, see *supra* note 91. Under the text of the current statute, "without authorization" is not defined. *See* 18 U.S.C. § 1030.

243. *See supra* notes 77, 79 and accompanying text.

244. *See supra* note 23 and accompanying text; *see also* Part I.A.

245. *See supra* notes 76–83 and accompanying text (discussing insiders versus outsiders under the CFAA).

246. *See supra* Parts I.B, II.

247. *See supra* Part I.B (explaining how the CFAA was intended to be an antihacking statute).

248. *See supra* Part II.

equipped to handle this evolving computer trend. Congress can remedy this by enacting an amendment to the CFAA that specifically targets outsiders and guides courts on how to treat cloud-computing systems under the law to resolve this unfair and unreasonable situation.