When is a Hack not a Hack: Addressing the CFAA's Applicability to the Internet Service Context

Laura Bernescu
Laura.Bernescu@chicagounbound.edu

Follow this and additional works at: http://chicagounbound.uchicago.edu/uclf

Recommended Citation
Bernescu, Laura () "When is a Hack not a Hack: Addressing the CFAA's Applicability to the Internet Service Context," University of Chicago Legal Forum. Vol. 2013: Iss. 1, Article 17.
Available at: http://chicagounbound.uchicago.edu/uclf/vol2013/iss1/17

This Comment is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in University of Chicago Legal Forum by an authorized administrator of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.
When is a Hack not a Hack: Addressing the CFAA's Applicability to the Internet Service Context

Laura Bernescu†

INTRODUCTION

Pew Research Center findings show that as of June 2012 approximately "[t]hree quarters . . . of Americans own either a desktop or laptop computer," while nearly nine out of every ten Americans own a cellphone. And more than half of cellphone owners use their cellphones to access the Internet. Along with such widespread Internet usage, typical consumers now also use a wider variety of Internet services on a daily basis, including online networking websites. Yet the legal issues potentially facing users of these Internet services continue to emerge and develop almost as fluidly as the world of social media itself.

Though the market has quickly adapted to the needs of the public, with new networking websites constantly popping up and

† BA 2011, Tufts University School of Arts and Sciences; JD Candidate 2014, The University of Chicago Law School.


3 Id.


providing users with opportunities to connect with like-minded individuals, the law has been slow to anticipate and respond to the legal issues introduced by the proliferation of such Internet services. Accordingly, courts are being asked to consider the scope of legal implications related to the use of networking websites and other Internet services. When it comes to the misuse of these websites in ways prohibited by the Terms of Service or other registration agreements, the federal law potentially applicable to these issues is the Computer Fraud and Abuse Act ("CFAA"), which governs "fraud and related activity in connection with computers." Yet the CFAA is almost twenty years older than the social networking giant Facebook, the online dating services eHarmony and Match.com, and the professional networking website LinkedIn. Considering the large generational gap between the enactment of the CFAA and the Internet services it governs, along with the fact that the Act has not been amended since 2008 (a time period during which the existence and breadth of Internet services has grown in

---

6 See, for example, Bannon, *State of the Media: The Social Media Report 2012* at 2 (cited in note 4) ("The number of social media networks consumers can choose from has exploded, and too many sites to count are adding social features or integration.")

7 For a discussion of some of the legal issues arising from the use of social networking sites, see generally Sharon Nelson, John Simek, and Jason Foltin, *The Legal Implications of Social Networking*, 22 Regent U L Rev 1 (2009). See also Fernando M. Pinguelo and Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals*, 16 Va J L & Tech 116, 188 (2011) (noting that “[law enforcement] in the cyber realm . . . has been largely reactive in nature”) (citation omitted).

8 See, for example, *PhoneDog v Kravitz*, 2012 WL 273323 *1 (ND Cal) (lawsuit over ownership and use of work related Twitter account).


10 18 USC § 1030.


12 Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn L Rev 1561, 1569 (2010) ("The most recent expansions to [the CFAA] were enacted in September 2008.").
leaps and bounds), it is evident that consumers, businesses, and legal professionals face uncertainty as to the legal consequences arising from the use of these websites and of other Internet services. And because the CFAA's current language is broad enough to "potentially regulate[] every use of every computer in the United States and even many millions of computers abroad," this uncertainty is not insignificant. As a result of this unsettled landscape, the practical reality for consumers is that little guidance exists in determining what may or may not be punishable misuse of Internet services; therefore, as consumers we must all tread cautiously and lightly whenever we click the "I Accept" button.

One source of uncertainty for consumers regarding the role of the CFAA in the Internet services context is that the meaning of the CFAA's language is unsettled. The CFAA establishes liability for access to computers and computer-based systems that is "without authorization" or that "exceeds authorized access." But from those two seemingly straightforward phrases, two significant legal disputes have arisen. First, several courts have attempted to distinguish between the two types of prohibited access—unauthorized access and excessive access—but have arrived at starkly different results that disagree not only about the meanings of the two phrases but also about the types of activities that may be considered unlawful under the CFAA. Second, a genuine circuit split exists over the meaning of the phrase "exceeds authorized access."

An additional wrinkle in the consumer/Internet services context is the fact that most of the "exceeds authorized access" litigation has been brought in the employment context, where an employer has sued a former employee for using the employer's data to start a competing business. As a result, much of the "exceeds authorized access" jurisprudence is nuanced by the common law of employer-employee relationships, rendering it

---

13 Id at 1561.
14 See 18 USC § 1030(a).
15 Compare International Airport Centers, LLC v Citrin, 440 F3d 418 (7th Cir 2006), with LVRC Holdings, LLC v Brekka, 581 F3d 1127 (9th Cir 2009).
16 Contrast United States v John, 597 F3d 263 (5th Cir 2010) and United States v Rodriguez, 628 F3d 1258 (11th Cir 2010), with LVRC Holdings, LLC v Brekka, 581 F3d 1127 (9th Cir 2009) and United States v Nosal, 676 F3d 854 (9th Cir 2012).
17 See, for example, Citrin, 440 F3d at 420–21 (defining an employee's CFAA
less than fully useful in the consumer context. Thus not only is the meaning of the language of the CFAA disputed among circuits, but many of the precedents and their reasoning are inapposite in the context of consumer usage of Internet services.

Lastly, at least one scholar has suggested that the CFAA has no applicability outside of the employment context because of the operation of the “void for vagueness” doctrine. According to Professor Orin Kerr, the use of the CFAA in the Internet services context is constitutionally deficient because it neither affords consumers with adequate notice, nor provides law enforcement with clear guidelines for enforceability.

Against that web of complexity, this Comment proposes a comprehensive resolution: by examining the legislative history of the CFAA and analyzing the existing CFAA case law, the Comment argues that the current language of the CFAA can be applied in the consumer Internet services context without creating an overly broad or unreasonably vague criminal statute. Specifically, this Comment takes the position that there is an interpretation of the phrase “exceeds authorized access” that is applicable to intentionally errant access to membership-required, Internet networking sites that have clear, well-defined Terms of Service. That interpretation of “exceeds authorized access” is consistent with the legislative history and the purpose of the CFAA and abides by the limitations imposed by the void for vagueness doctrine.

Part I of this Comment elaborates on the background of the CFAA from its initial enactment to its subsequent amendments. Part II presents the relevant case law, addressing both the struggle over differentiating “without authorization” and “exceeds authorized access,” and the “exceeds authorized access” circuit split. Part III discusses the more recent applications of the CFAA to the Internet services context. Part IV analyzes the viability of the different CFAA approaches in the Internet services context, and Part V proposes limiting principles to ensure that the CFAA can withstand void for vagueness challenges in the Internet service context. Finally, Part VI

liability in terms of the duty of loyalty owed by the employee as the employer’s agent).

18 See generally Kerr, 94 Minn L Rev 1561 (cited in note 12). The void for vagueness doctrine requires that courts define laws both clearly and narrowly so as to provide notice to the public of what behavior is potentially punishable and to ensure that law enforcement is constrained from imposing laws discriminately. Id at 1575.

19 Id at 1561.
concludes by summarizing the factual background, the relevant arguments, and the proposed solution to the issue discussed herein.

I. THE CFAA AND ITS LEGISLATIVE HISTORY

At the start of the 1980's, the American public began to perceive a new type of criminal threat: the computer hacker. Due, in part, to the growing availability of "inexpensive personal computers[,] . . . the dramatic growth of computer literacy, . . . and [ ] the introduction of the computer network," hacking became both more accessible and more feared, and, as a result, hackers gained prominence and infamy. Popular media also helped bring the issue of computer hacking to the public's consciousness with the 1983 film, War Games, which "provid[ed] a point of cultural reference regarding the dangers of computers and their users." Against this backdrop, legislators felt compelled to act.

As an initial response to concerns about computer hacking, Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. At that time, § 1030 of that act criminalized certain actions committed by a person who "knowingly accessee[d] a computer without authorization, or having accessed a computer with authorization, use[d] the opportunity such access provide[d] for purposes to which such authorization did not extend." Under that 1984 version of § 1030, a person meeting one of the scienter-based access requirements was subject to criminal liability in three scenarios. Specifically, the 1984 version of § 1030(a) read as follows:

---

21 Id at 66.
23 HR Rep No 98-894, 98th Cong, 2d Sess 1984 (1984), reprinted in 1984 USCCAN 3689 (citing the War Games depiction of computer hacking as a reference point for the dangers to which Congress had to respond in its proposal to criminalize computer-related crimes).
24 Counterfeit Access Act of 1984, 98 Stat 2190. See also HR Rep No 98-894, 98th Cong, 2d Sess 1984 (1984), reprinted in 1984 USCCAN 3689 (noting the lack of federal legislation dealing with computer crimes and the need for such legislation in light of the emergence of hackers taking advantage of increased "computer networking").
(a) Whoever—

(1) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information contained in a financial record of a financial institution, . . . or contained in a file of a consumer reporting agency on a consumer . . . ; or

(3) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;

shall be punished[.]²⁶

Succinctly summarized, the three scenarios in which the 1984 CFAA criminalized computer access without or beyond authorization were "misuse to obtain national security

²⁶ 18 USC § 1030(a) (Supp II 1985).
secrets, . . . [misuse] to obtain personal financial records, and hacking into U.S. government computers."\(^{27}\)

Two years later, Congress expanded the list of federal computer crimes enumerated in the CFAA by enacting the Computer Fraud and Abuse Act of 1986.\(^{28}\) Specifically, Congress added three new scenarios under which persons could face CFAA liability.\(^{29}\) These new scenarios were codified at § 1030(a)(4)–(6), which read in 1986 as follows:

(a) Whoever—

. . .

(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ;

(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct, alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information and thereby—

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

(B) modifies or impairs . . . the medical care of one or more individuals; or

(6) knowingly and with intent to defraud traffics . . . in any password . . . through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

---

\(^{27}\) Kerr, 94 Minn L Rev at 1564 (cited in note 12).

\(^{28}\) Pub L No 99-474, 100 Stat 1213, amending 18 USC § 1030 ("Computer Fraud and Abuse Act").

\(^{29}\) Computer Fraud and Abuse Act § 2(d), 100 Stat at 1213–14.
(B) such computer is used by or for the Government of the United States; shall be punished[.]

Most importantly for the purpose of this Comment, Congress replaced the "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" language in the 1984 version of § 1030(a)(1), (2), and (3) with the words "or exceeds authorized access." The new "exceeds authorized access" language, which phrase was defined to mean "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 to obtain or alter," was also incorporated into the new § 1030(a)(4) offense. To this day, the "exceeds authorized access" language remains unchanged in those sections of the CFAA. The Senate Report from the time of this amendment indicates that the Committee on the Judiciary intended this change to clarify "one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization."

In 1994, Congress further expanded the reach of the CFAA by establishing a private right of action for individuals harmed by certain violations of the CFAA. That private right of action

---

30 18 USC § 1030(a)(4)–(6) (1982 and Supp IV 1987). The 1986 enactment limited several of the new § 1030(a) violations to "Federal interest computer[s]," defined as computers used by the United States Government or by a financial institution or as two or more computers involved in an "interstate offense over an interstate network." Computer Fraud and Abuse Act § 2(d), (g), 100 Stat at 1213–15, codified at 18 USC § 1030(a)(4)–(5), (e)(2) (1982 and Supp IV 1987).


32 Computer Fraud and Abuse Act § 2(g), 100 Stat at 1215, codified at 18 USC § 1030(e)(6) (1982 and Supp IV 1987).

33 Computer Fraud and Abuse Act § 2(d), 100 Stat at 1213.

34 See 18 USC § 1030.

35 S Rep No 99-432 at 21 (cited in note 31).

exists in its current form at § 1030(g). Through the use of the CFAA's civil provision, persons responsible for authorizing computer use are able to police authorized users and bring suits for damages arising from violations of authorized use, both through access without authorization and access exceeding authorization. Many of the cases contributing to the CFAA jurisprudence were brought under the § 1030(g) private right of action, usually in the employment context. Indeed, employment-related computer use is a clear example of when an employer-authorizer can impose strict limits on an employee-user's access.

Additional amendments throughout the 1990s and 2000s expanded the scope of the CFAA by extending the applicability of certain CFAA violations to the ever-expanding category of "protected computers." The CFAA's current definition of "protected computers" covers both computers used by the United States Government or financial institutions, as originally intended by the drafters of § 1030, and computers "used in or affecting interstate or foreign commerce or communication." The remaining CFAA violations apply to all "computers," which, as defined means "any high speed data processing device... and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but... does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." Thus, the CFAA

37 See 18 USC §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.").
38 18 USC § 1030(g). See also Andrew T. Hernacki, Comment, 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, 1551–52 (2012).
39 See, for example, United States v Nosal, 676 F3d 854, 860 n 6 (9th Cir 2012) (noting employers' use of the "CFAA against employees in civil cases").
40 18 USC § 1030(e)(2)(B) (Supp II 1995) (introducing the "protected computers" language); 18 USC § 1030(e)(2)(B) (Supp II 2004) (enlarging the definition of "protected computers" to reach computers outside of the United States); 18 USC § 1030(e)(2)(B) (Supp II 2009) (modifying the definition of "protected computers" to encompass not just computers used in intrastate and foreign commerce but also computers "affecting" interstate and foreign commerce).
41 See 18 USC § 1030 (Supp II 1985).
42 18 USC § 1030(e)(2).
43 18 USC § 1030(e)(1).
44 18 USC § 1030(e)(1) (defining "computer").
applicability extends beyond commonly considered devices like personal computers, desktops, and laptops. By incrementally expanding both the scope of devices and the uses of such devices governed by the CFAA, Congress effectively ensured that any device with access to the Internet, regardless of whether it is actually used in interstate commerce, is governed by the CFAA.45

Today, the expanded language of the CFAA imposes liability in the following circumstances:

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined... to require protection against unauthorized disclosure... willfully communicates, delivers, transmits, ... the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, ... or contained in a file of a consumer reporting agency on a consumer, ... ;

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

... 

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct

45 Kerr, 94 Minn L Rev at 1570–71 (cited in note 12) ("[The new definition of 'protected computers'] does not merely cover computers connected to the Internet that are actually 'used' in interstate commerce. Instead, it applies to all computers, period, so [far as the Commerce Clause will allow].") (citations omitted).
further the intended fraud and obtains anything of value . . . ;

. . . shall be punished[.]\(^{46}\)

As evident from the language above, the two types of liability under § 1030(a)(1), (2), and (4) are when a user gains access without authorization and when an authorized user exceeds authorized access.\(^{47}\) Although the term “exceeds authorized access” is defined in the statute,\(^{48}\) the difference between those two types of violations is not obvious. Indeed, several courts have struggled to pair putatively illegal activities with the appropriate type of CFAA liability.\(^{49}\) However, one portion of the legislative history of the CFAA begins to illuminate the difference between the types of activities prohibited by the CFAA’s “exceeds authorized access” provision and the types of activities prohibited by the “without authorization” provision. The Senate’s Judiciary Committee post-enactment report on the 1994 amendments to the CFAA indicates that the distinction between the two provisions was understood by the Committee to rest on the user’s affiliation with the computer in question.\(^{50}\) Under this interpretation, an outside user who gains access to a computer through clandestine means, such as “deliberately break[ing] into a computer,” would be liable for accessing a computer “without authorization”; while an inside user who has authorization to access a computer but surpasses the confines of that authorization by “obtain[ing] or alter[ing] information in the computer that [he] is not entitled so to obtain or alter” would be liable for “exceeding authorized access” to the computer.\(^{51}\)

\(^{46}\) 18 USC § 1030(a)(1), (2), (4).

\(^{47}\) 18 USC § 1030(a)(1), (2), (4).

\(^{48}\) See 18 USC § 1030(e)(6) (“[T]he term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.”).

\(^{49}\) See notes 53–59 and accompanying text.


\(^{51}\) S Rep No 104-357 at 6, 21 (cited in note 50).
II. CFAA CASE LAW

The legal consequences for violating the CFAA are not trivial: individuals convicted of a CFAA violation face penalties of between one and ten years in prison. But the law is far from settled, and this confusion breeds uncertainty for consumers who may use Internet social networking services and other Internet services in violation of the Terms of Service. The importance of correctly defining “without authorization” and “exceeds authorized access” is twofold. First, determining the respective definitions of the two phrases will help identify within which category an indictable activity should be analyzed. And second, defining the two forms of liability more precisely will help highlight which activities the CFAA may reach at all. Accordingly, understanding what activities trigger what types of liability under the CFAA, as well as whether certain activities can even be reached by the CFAA, will clarify the law to protect legitimate computer use while guarding against the kind of abuses that the CFAA was intended to address.

A. Distinguishing “Without Authorization” From “Exceeding Authorized Access”

Determining that a user acted “without authorization” is fairly simple where that user hacked into or otherwise accessed a computer that he had no permission or right to access. In United States v Ivanov, for example, the court easily found that a foreign hacker who accessed a company’s computers and took possession of its data acted “without authorization” under the CFAA. Because the perpetrator of the unauthorized access, a Russian hacker, was completely unaffiliated with the Connecticut online financial clearinghouse whose computers he accessed, “[took] complete control over [their] data, and consequently, had possession of it,” the court almost automatically determined that he violated the CFAA’s “without authorization” provision.

53 175 F Supp 2d 367 (D Conn 2001).
54 Id at 371–72.
55 Id.
However, courts have historically had trouble determining whether an individual "exceed[ed] authorized access" or acted "without authorization" when the individual had limited authorization to access a computer and its data but exceeded that authorization in some way. For instance, in *International Airport Centers, LLC v Citrin*, the Seventh Circuit held that an employee who had been authorized to access his employer's computers nonetheless accessed those computers "without authorization" after the employee lost his authorization. Consequently, the court determined that the employee breached his duty of loyalty to his employer when he violated his employment contract by starting a competing business and permanently deleting files on the employer's computers, against the employer's interests. Because the agency relationship between the employer-principal and the employee-agent was terminated by the employee's breach, the Seventh Circuit reasoned that the employee lost his authorization to access the employer's computers and concluded that he, most likely, acted "without authorization."

Interestingly, the Seventh Circuit in *Citrin* only fleetingly considered the distinction between "exceeds authorized access" and "without authorization." While the court briefly struggled to distinguish the two phrases, it ultimately determined the distinction to be "paper thin" and, as explained above, relied instead on the duty of loyalty inherent in an agency relationship to determine the limits of the employer's access.

Other courts have been reluctant to apply the Seventh Circuit's holding in *Citrin* to similar employment contexts. For example, the Ninth Circuit in *LVRC Holdings, LLC v Brekka* explained that *authorization* within the meaning of the CFAA depends not on the user's actions with respect to the computer

---

56 440 F3d 418 (7th Cir 2006).
57 Id at 420–21.
58 Id at 419.
59 440 F3d at 421. The Seventh Circuit considered this case on appeal after the plaintiff's suit was dismissed by the trial court. As such, the court did not reach any definitive conclusions on the questions of fact, but rather reversed the dismissal, reinstated the suit, and remanded it to the trial court.
60 Id at 420.
61 *LVRC Holdings, LLC v Brekka*, 581 F3d 1127 (9th Cir 2009). See also *WEC Carolina Energy Solutions LLC v Miller*, 687 F3d 199 (4th Cir 2012).
62 581 F3d 1127 (9th Cir 2009).
and data he is authorized to access but rather on the authorizing party’s actions. In *Brekka*, the court held that an employee of an operator of residential treatment centers did not violate the CFAA when he emailed company documents to his private computer and continued to access the company’s web-marketing statistics even after terminating his employment. Notably, the employee “did not have a written employment agreement, nor did [the employer] promulgate employee guidelines that would prohibit employees from emailing [company] documents to personal computers.” The court reasoned that a user cannot be liable under the CFAA’s “without authorization” provision unless the authorizing party—usually the user’s employer—has expressly withdrawn the user’s authorization to access the computers and data before the user undertakes the contested actions. Because the employee in that case was authorized to access the information at issue since he had been given permission to use the company’s computers, he could not have acted “without authorization.” Thus, according to the *Brekka* court, if the authorizing party cannot show that it explicitly withdrew a user’s authorization, the case against the user who is authorized access “for certain purposes but goes beyond those limitations” must be pursued under the “exceeds authorized access” provision of the CFAA.

The Ninth Circuit also rejected the application of duty of loyalty and agency principles to determine authorization and criticized the Seventh Circuit for taking such an expansive and novel interpretation of a criminal statute. According to the *Brekka* court, the approach in *Citrin* neither “comported with the plain language of the CFAA, . . . [nor provided] defendant [with sufficient] notice as to which acts” could be punishable under the statute.

The *Brekka* approach is different from the Seventh Circuit’s approach because it vehemently rejects the notion, embraced by

---

63 Id at 1133–34.
64 Id at 1130, 1136.
65 Id at 1129.
66 *Brekka*, 581 F3d at 1133.
67 Id.
68 Id.
69 Id at 1135.
70 *Brekka*, 581 F3d at 1135.
the Citrin court, that a user’s actions alone can bring him within the scope of the CFAA’s “exceeds authorized access” provision. Indeed, under the Brekka approach, a user cannot be liable for access without authorization until the authorizing party clearly “rescind[s] the [user’s] right to use the computer.” Thus, the Brekka approach tends to push more cases into the “exceeds authorized access” version of CFAA liability. Proceeding under the “exceeds authorized access” provisions of the CFAA, however, comes with its own set of problems, which are exemplified by a recently developed circuit split.

B. The “Exceeds Authorized Access” Circuit Split

1. Intended use analysis.

The Fifth Circuit addressed the meaning of the phrase “exceeds authorized access” in United States v John and focused on the use for which the authorized user’s access was intended. In John, the government prosecuted a former employee of a financial institution for “exceeding authorized access to a protected computer” to obtain financial information in violation of § 1030(a)(2). The employee had used her access to the institution’s internal computer system to provide a third party with customer account information that was subsequently used to incur fraudulent charges. After being convicted at the trial court level, the employee argued on appeal that she was in fact authorized to access the customer account information and therefore could not have exceeded her authorized access level. The Fifth Circuit rejected the employee’s contention, holding that an employee who uses information beyond its intended use exceeds authorized access. Generally, the court noted, “the scope of a user’s authorization to access a protected computer [is determined] on the basis of the expected norms of intended use or the nature of the relationship established between the

71 Id.
72 597 F3d 263 (5th Cir 2010).
73 Id at 271.
74 Id at 270.
75 Id.
76 John, 597 F3d at 271.
77 Id at 272.
computer owner and the user.”

Here, the employer-employee relationship, along with the employer’s official policy, “prohibit[ing] misuse of the company’s internal computer systems and confidential customer information,” defined the scope of the employee’s authorization. Thus, while the employee was authorized to access the customer account information for legitimate employment-related purposes, she was not authorized to access it “for any and all purposes.”

Because the employee had “reason to know that... she [was] not authorized to access data or information in furtherance of a criminally fraudulent scheme,” the court found that she had exceeded authorized access in violation of the CFAA.

In United States v Rodriguez, the Eleventh Circuit also considered the meaning of “exceeds authorized access.” Seemingly agreeing with the Fifth Circuit, the Eleventh Circuit applied its own variation of the intended use analysis. In Rodriguez, a former employee of the Social Security Administration used his access to the Administration’s database to access the personal information of over a dozen individuals for reasons unrelated to his job. Like the employee in John, the employee argued on appeal that his access was authorized because he had access to the information in the ordinary course of his job. Taking the same approach as the Fifth Circuit, the Eleventh Circuit concluded that because the employee had been told that “he was not authorized to obtain information for nonbusiness reasons,” he exceeded his authorized access when he accessed the information in violation of that policy.

Going further, the Rodriguez court distinguished between situations in which an employee violates a clear policy delineating the proper use of accessed information—which, as was the case in Rodriguez, result in “exceeds authorized access” liability—and...
situations in which no such policy exists. In the second class of scenarios—where no clear policy on use of electronically accessed information exists—the Fifth Circuit implied that the Ninth Circuit's approach in *Brekka* was correct in finding that the employee there did not violate the CFAA.88

In summary, both the Fifth and Eleventh Circuits focus on the nature of the relationship between the authorizing party (in the cases, an employer) and the authorized party (an employee), with regard to workplace norms and the resulting policies, in order to determine the scope of the authorization. Because employment establishes a relationship between the employer and employee, policies can easily embody the expected norms of acceptable and permissible employee behavior. The employee in *John* exceeded the scope of her authorization because she used her authorized access in a way that was beyond the expected norms of the employer-employee relationship upon which the employer's policy was based; the employee in *Rodriguez* exceeded the scope of his authorization because he used his authorized access for a purpose other than conducting his duties as an employee, a norm embodied in his employer's policy. This approach, which interprets the phrase "exceeds authorized access" in reference to the reason for the authorization, can be characterized as intended use analysis.

2. The narrower approach.

Other courts, however, have rejected the intended use approach. In *EF Cultural Travel BV v Zefer Corporation*,89 a corporation sued its competitor for using a "scraper tool"—"a computer program that accesses information contained in a succession of webpages stored on the accessed computer"—to collect pricing information from the corporation's publicly accessible website.90 On appeal, the First Circuit refused to analyze the expected norms between the two unaffiliated parties in order to determine the scope of the competitor's authorization to access the public website.91 Instead, the court held that because the corporation could easily use explicit terms to define

88 Id. See also text accompanying notes 62–71.
89 318 F3d 58 (1st Cir 2003).
90 Id at 60–61.
91 Id at 63.
the scope of authorized access to its website and notify users of those terms, the court would not infer implicit limits to the public website's use.92 "[P]ublic website provider[s] can easily spell out explicitly what is forbidden," so there is no need for a court to put public "users at the mercy of a highly imprecise, litigation-spawning standard like 'reasonable expectations'" on the limits of authorization.93

Even within the employment context, some courts have moved away from the intended use analysis. For example, although the Ninth Circuit in Brekka court determined that the defendant employee did not act "without authorization" when he emailed company documents to himself and continued to access the company's online information even after terminating his employment,94 the court also considered the employer's implicit argument that the defendant employee "exceeded authorized access" in violation of Section 1030(a)(2), (4).95 The court criticized the broad interpretation of "exceeds authorized access."96 Specifically, the court refused to read an intended use requirement into the CFAA's "exceeds authorized access" provision because it found no support for such a requirement in the definition of "exceeds authorized access" or in the language of the CFAA as a whole.97 The court reasoned that, even in the civil context, the CFAA should be construed narrowly so as to ensure that it does not "impose unexpected burdens on defendants."98 The court concluded that the only sensible approach to "exceeds authorized access" was as a reference to someone who "has permission to access the computer but accesses information on the computer that [he] is not entitled to access," rather than as a reference to the reason for the authorization.99 Thus, because the defendant employee was authorized, as part of his employment, to access both the

92 Id at 62.
93 EF Cultural Travel, 318 F3d at 63.
94 See notes 62–70 and accompanying text.
95 Brekka, 581 F3d at 1135 & n 7. The employer's charge that the employee "exceeded authorization" was considered an implicit argument because on appeal to the Ninth Circuit the employer only argued that the employee acted "without authorization." Id at 1135 n 7.
96 See id at 1133–35.
97 Id at 1133–34.
98 Id at 1134–35.
99 Brekka, 581 F3d at 1133.
computer and the information, he was not liable for an "exceeds authorized access" violation.\textsuperscript{100}

The Ninth Circuit affirmed its denunciation of the expansive intended use approach to "exceeds authorized access" cases in its en banc rehearing of \textit{United States v Nosal}.\textsuperscript{101} In \textit{Nosal}, the government prosecuted employees of an executive search firm for violating § 1030(a)(4) of the CFAA after they downloaded information from a confidential database and transferred that information to a former employee who was in the process of starting a competing business.\textsuperscript{102} Although the employees were authorized to access the database, their access was limited exclusively for the firm's business.\textsuperscript{103} Initially, the district court rejected the defendant employees' motion to dismiss the CFAA charges based on a narrow construction of § 1030.\textsuperscript{104} However, the defendant employees tried again shortly after, filing both a motion to dismiss and a motion for reconsideration, on the basis of the Ninth Circuit decision in \textit{Brekka}.\textsuperscript{105} This time, the district court agreed with the defendant employees and dismissed the CFAA charges,\textsuperscript{106} but the Ninth Circuit reversed and remanded once the government appealed.\textsuperscript{107} Subsequently, the Ninth Circuit granted a rehearing en banc.\textsuperscript{108}

At the en banc rehearing, the Ninth Circuit was faced with the government's argument that the scope of "exceeds authorized access" should be determined by reference to the permissible use of authorization; nevertheless, the Ninth Circuit held that "exceeds authorized access . . . does not extend to violations of use restrictions" and dismissed the CFAA charges against the employees.\textsuperscript{109} In arriving at that decision, the Ninth Circuit chose between two competing approaches to the meaning of "exceeds authorized access": (1) "someone who is authorized to

\textsuperscript{100} \textit{Id} at 1135, 1129.
\textsuperscript{101} \textit{676 F3d} 854 (9th Cir 2012).
\textsuperscript{102} \textit{Id} at 856 & n 1.
\textsuperscript{103} \textit{Id}.
\textsuperscript{104} \textit{United States v Nosal}, 2009 WL 981336, *7 (ND Cal).
\textsuperscript{105} \textit{Nosal}, \textit{676 F3d} at 856.
\textsuperscript{106} \textit{United States v Nosal}, 2010 WL 934257, *9 (ND Cal).
\textsuperscript{107} \textit{United States v Nosal}, 642 F3d 781, 791 (9th Cir 2011).
\textsuperscript{108} \textit{Nosal}, \textit{676 F3d} at 856.
\textsuperscript{109} \textit{Id} at 863–64.
access only certain data or files but accesses unauthorized data or files”; or (2) "someone who has unrestricted access to a computer, but is limited in the use to which he can put the information.”\textsuperscript{110} The court rejected the second definition, and therefore the intended use approach, because it improperly "transform[ed] the CFAA from an anti-hacking statute into an expansive misappropriation statute,” an expansion the court found improper without clear congressional intent.\textsuperscript{111} The court was also satisfied that the first approach—that “someone who [was] authorized to access only certain data or files but accesse[d] unauthorized data or files” has “exceeded authorized access”—maintained the distinction between “exceeds authorized access” and “without authorization” by focusing on the extent of the access rather than its use. Moreover, the court found that approach to be consistent with the congressional understanding, evidenced in the legislative history, of the distinction as one between insider users and outsider users.\textsuperscript{112}

Noting the expansive definition of “protected computers” under the CFAA, the \textit{Nosal} court also expressed concerns about the scope and breadth of the CFAA outside of the employment context by observing that “the [broad] interpretation of 'exceeds authorized access' makes every violation of a private computer use policy a federal crime.”\textsuperscript{113} The court then described a plethora of innocuous activities that might become federal crimes if the broad, intended use approach to “exceeds authorized access” was universally adopted, including lying on an online dating profile and posting “inappropriate materials” for sale on eBay—a practice prohibited by the eBay User Agreement but lacking an explanation of what is and is not appropriate.\textsuperscript{114} Thus, while the court conceded that minor violations would likely not be prosecuted under the CFAA, it refused to interpret “exceeds authorized access” in a way that would require the public “to live at the mercy of [the] local prosecutor.”\textsuperscript{115}

\textsuperscript{110} Id at 857.
\textsuperscript{111} Id.
\textsuperscript{113} \textit{Nosal}, 676 F3d at 859.
\textsuperscript{114} Id at 861–62.
\textsuperscript{115} Id at 862.
Further demonstrating the controversy involved in the phrase “exceeds authorized access,” two judges dissented from the en banc decision in Nosal. Disagreeing with the narrow definition adopted by the majority, the dissent argued that the intended use analysis employed by the Fifth and Eleventh Circuits should be adopted.\footnote{Nosal, 676 F3d at 865 (Silverman and Tallman dissenting).} In the dissent’s view, the intended use analysis was supported and contemplated by the plain language of the CFAA and its definition of “exceeds authorized access.”\footnote{Id.} The dissenters were also critical of the “parade of horribles” presented by the majority as support for a narrow reading of “exceeds authorized access.”\footnote{Id at 866.}

III. RECENT CFAA DEVELOPMENTS IN THE INTERNET SERVICE CONTEXT

A. United States v Drew

In 2006, Lori Drew created a fake MySpace profile, pretending to be an attractive teenage boy, and used it to contact Megan Meier, a former friend of Drew’s teenage daughter.\footnote{Indictment, United States v Drew, CR08-00582, *6-8 (CD Cal filed May 15, 2008) (available on Westlaw at 2008 WL 2078622) (“Drew Indictment”). See also United States v Drew, 259 FRD 448 (CD Cal 2009).} Over the course of two months, Drew continued the ruse, while Meier and the fictional boy developed a deep relationship.\footnote{Id.} Then, after the fictional boy suddenly rejected Meier, telling her in a message that that “the world would be a better place without [her],” Meier hanged herself and died.\footnote{Id.}

The government prosecuted Drew under § 1030(a)(2)(C) and § 1030(c)(2)(B)(ii)\footnote{Section 1030(c)(2)(B)(ii) of the CFAA imposes a fine and a maximum prison term of five years for offenses under § 1030(a)(2).} of the CFAA for creating a MySpace profile in violation of the MySpace Terms of Service.\footnote{Drew Indictment at *9–10.} Because the MySpace Terms of Service prohibited creating a fake profile, the government contended that Drew “intentionally accessed MySpace’s computer/servers without authorization and/or in
excess of authorization” in violation of the CFAA.\textsuperscript{124} When a jury convicted Drew, she moved for a judgment of acquittal.\textsuperscript{125} The trial court conceded that the owner of a website is permitted to dictate the “limitations[,] restrictions[, and ] conditions” placed on users of the website, but ultimately concluded that the MySpace Terms of Service were an inadequate basis for criminal liability.\textsuperscript{126} Accordingly, the court granted Drew’s motion for acquittal.\textsuperscript{127}

Initially, the court concluded that an intentional breach of the Terms of Service could “potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the [CFAA]” because the owner of a website may properly define the conditions and limitations on access to his website.\textsuperscript{128} Nevertheless, the court refused to extend criminal liability under the Terms of Service because doing so would render the CFAA void under the constitutional vagueness doctrine.\textsuperscript{129} The void for vagueness doctrine requires that statutes be sufficiently specific so that the public has notice of what activity the law criminalizes and law enforcement has clear guidelines to determine the application of the law.\textsuperscript{130}

The court first addressed the notice requirement and found that the CFAA did not explicitly, or implicitly, criminalize breaches of contract, and even if it did, basing CFAA violations on a Terms of Service agreement would be “unacceptably vague.”\textsuperscript{131} The court anticipated further vagueness issues arising from allowing website owners to define criminal conduct through the Terms of Services; this was especially troubling to the court since Terms of Service tend to be vague and website owners often retain the right to unilaterally alter them.\textsuperscript{132} Additionally,
the court predicted that complications would arise from applying "contractual requirements within the applicable [T]erm of [S]ervice to [ ] criminal prosecution[s]." The court then confronted the guidelines for law enforcement requirement and held that even if "[a] conscious breach of a website's [T]erms of [S]ervice is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that [the CFAA] becomes a law 'that affords too much discretion to the police.'" Ultimately, the court held that because the CFAA does not adequately describe the type of activity it criminalizes such that "individuals of 'common intelligence' are on notice that a breach" of such terms is a crime, applying the CFAA in the Terms of Service context would not be sufficiently clear for criminal liability to attach.

Notably, the court in Drew was unclear about whether enforcement of the CFAA based on Terms of Service violations would always, under any circumstances, cause adequate notice and guidelines for law enforcement issues under the void for vagueness doctrine. The court did not clarify whether the CFAA is vague as applied to the limited facts it was considering, or whether it is always vague when applied to Terms of Service even if the troubling characteristics the court flagged in MySpace's Terms of Service were eliminated.

B. Aaron Swartz

The 2013 suicide of Internet activist Aaron Swartz brought the CFAA back into the media spotlight. In 2009, Swartz, a computer programmer and open-government activist, used a free trial of the government-run Public Access to Court Electronic Records (PACER) system to download almost 20 percent of the documents in the database, which he

---

133 Id.
134 Id at 467, citing City of Chicago v Morales, 527 US 41, 64 (1999).
135 Drew, 259 FRD at 464.
136 See, for example, Zach Carter, Ryan Grim, and Ryan J. Reilly, Aaron Swartz, Internet Pioneer, Found Dead Amid Prosecutor 'Bullying' In Unconventional Case (Huffington Post Jan 12, 2013), online at http://www.huffingtonpost.com/2013/01/12/aaron-swartz_n_2463726.html (visited Sept 15, 2013); Noam Cohen, A Data Crusader, a Defendant and Now, a Cause, NY Times A1 (Jan 14, 2013).
subsequently openly posted online. The Federal Bureau of
Investigations was unable to find any illegality in Swartz’s
actions and closed its investigation in April 2009.

Less than two years later, Swartz again caught the
attention of law enforcement. This time, the government
managed to indict Swartz for alleged misuse of the online
database JSTOR, which “provides an online system for archiving
and providing access to academic journals and journal
articles.” Swartz had valid access to JSTOR because he was a
fellow at Harvard University. Although Swartz was not
affiliated with the Massachusetts Institute of Technology (MIT),
he used guest access to MIT’s computer network to download 4.8
million documents from JSTOR over a period of almost five
months. During the five-month period, Swartz repeatedly
thwarted attempts by both MIT and JSTOR to restrict his
ability to download documents from the JSTOR database; for
example, by using multiple computers, establishing new IP
addresses, and changing MAC addresses.

Swartz was charged with various computer-related crimes,
including “[u]nlawfully [o]btaining [i]nformation from a
[p]rotected [c]omputer” under § 1030(a)(3), one of the CFAA’s
“unauthorized access” provisions. The charges against Swartz
exposed him to potential sanctions of up to thirty-five years in
prison and millions of dollars in fines. Swartz committed
suicide in January 2013, which some commentators have

137 John Schwartz, An Effort to Upgrade a Court Archive System to Free and Easy, NY Times A16 (Feb 13, 2009).
140 Id at *3.
143 Swartz Indictment at *13.
attributed to pressures caused by prosecutorial overreaching.\footnote{145}{See, for example, Lawrence Lessig, \textit{Prosecutor as Bully} (Lessig Blog Jan 12, 2013), online at http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully (visited Sept 15, 2013).}

In any event, legal experts, and politicians have started to take a closer look at the CFAA and its implications for the everyday use of online services.\footnote{146}{See, for example, Kim Zetter, \textit{Congress Demands Justice Department Explain Aaron Swartz Prosecution} (Wired Jan 29, 2013), online at http://www.wired.com/threatlevel/2013/01/doj-briefing-on-aaron-swartz/ (visited Sept 15, 2013).}

As the Lori Drew and Aaron Swartz cases demonstrate, the CFAA is extremely broad and can possibly be interpreted in a way that potentially criminalizes the behavior of any individual who uses a computer device with the capability to connect to the Internet in a way that is contrary to what a website’s owner deems permissible. Certainly, Lori Drew’s actions and their consequences are morally deplorable, however, until we can distinguish and narrow CFAA liability to only reach the type of behavior she engaged in, and avoid potentially criminalizing even the most innocuous violations of a website’s Terms of Service, we should be wary of the application of the CFAA outside of the employment context. Therefore, the proper definition of any of the terms integral to determining liability under the CFAA—including “without authorization” and “exceeds authorized access”—is critical to understanding the application of the CFAA in the Internet service context.

IV. THE APPLICABILITY OF EXISTING CFAA JURISPRUDENCE TO THE INTERNET SERVICE CONTEXT

In light of the legal regime discussed above—including the latent circuit split over the meaning of the phrase “exceeds authorized access” and the government’s increasingly aggressive use of the CFAA—can the CFAA be applied outside the employment context without extending liability to harmless behavior? In answering that question, this Comment provides a fuller understanding of the ways in which the CFAA can be held applicable to Internet services that require a user to register and acquiesce to certain terms prior to using the service. This analysis is important for two reasons. First, social networking sites are increasingly popular and it is important that users understand the legal ramifications of joining such sites. Second,
violations of the CFAA are punishable by a range of means from monetary fines or damages to imprisonment. Together, these two realities make for a volatile environment in which a vast number of Internet services users are unaware and uncertain of what may constitute culpable behavior or what the consequence of that behavior could be. This Comment tries to bring some clarity and predictability to this environment by suggesting guidelines for the application of the CFAA in the Internet services context.

A. Meaning of “Exceeds Authorized Access” vs “Without Authorization”

In the Internet services context, as in the employment context, the first order question is whether a user’s access exceeded authorization or was without authorization. Thus, the first step in understanding the applicability of the CFAA in the non-employment context is to properly distinguish between consumer situations in which access is undertaken “without authorization” and those in which use “exceeds authorized access.” The distinction between the two scienter-based access requirements must be maintained in order to remain true to the legislative intent that animated the inclusion of both phrases in the language of the CFAA.

1. Rejecting the Seventh Circuit.

The interpretation employed by the Seventh Circuit in Citrin—that a user who previously received authorization to use a computer can be liable for a “without authorization” violation if such authorization is impliedly rescinded following a breach of a duty owed to the authorizing party—should not be extended to the consumer context. That approach is inconsistent with the plain language of the CFAA because it completely eradicates any distinction between the two scienter-based access requirements and renders the inclusion of “exceeds authorized access” redundant. If any user who acts outside of his authorized access is treated as acting “without authorization,” there is no scenario under which he would be liable for exceeding authorized

147 See notes 56–60 and accompanying text.
access rather than accessing a computer system without authorization.

The Seventh Circuit's approach to "without authorization" is also problematic in the Internet services context because it introduces common law elements into the CFAA that are inapplicable outside of the employment context. Specifically, this approach is based on the duty inherent in the relationship of agency between the employer-authorizer and the employee-user. Since the law has not recognized a similar agency relationship between an Internet service provider and an Internet service user, the rationale is inoperative in the consumer context. Accordingly, the Seventh Circuit's approach to "without authorization" and "exceeds authorized access" cannot be used in the Internet service context because it neither provides a basis for defining the authorization in the Internet user-authorizer, nor distinguishes between violations "without authorization" or "exceeding authorized access."

2. Accepting the Ninth Circuit.

Instead, the clearer and more straightforward approach to the distinction between "without authorization" and "exceeding authorized access," supported by the Ninth Circuit in Brekka and Nosal, should be extended to the Internet services context. In those cases, the Ninth Circuit suggested that an authorized user who utilizes his access beyond the limits of his authorization has "exceed[ed] authorized access," while a user who has no permission to access a computer system or whose authorization to access a computer system has been expressly revoked has acted "without authorization."148 This approach is appropriate, particularly in the non-employment context, because it is consistent with the CFAA's original purpose—to combat technical computer hacking.149 It also preserves the distinction between the two scienter requirements by respecting the original inside user versus outside user understanding of those requirements.150 Indeed, in the Internet services context,
this interpretation will result in liability under the CFAA's "without authorization" provisions only in the traditional situations of hacking into a computer to which a user does not have authorization by such means as using code to get past protections intended to keep unauthorized users out or improperly using another's password.

Under the Ninth Circuit's approach, an Internet services user would be liable if, before receiving authorization to access the service or after any such authorization has been clearly rescinded, he uses technical computer knowledge to access the service's data. For example, if a networking website requires users to register before accessing content and a user finds a way to access the content without registering or to continue accessing the content after his registration has been revoked, the user has accessed information "without authorization." Similarly, if one registered and authorized user of an Internet service uses another user's password and account to access the service, the first user has accessed information "without authorization" because he was never received permission to access the service as another user. At first glance, this interpretation in the non-employment context might seem overly broad, since a user might easily access protected information by mistake. The CFAA, however, limits liability to users who "knowingly" or "intentionally" access a computer.15 Thus, individuals who unintentionally stumble upon access to information that is protected by some form of registration will not be penalized.

B. Meaning of "Exceeds Authorized Access"

The second step in determining the applicability of the CFAA in the non-employment context is to understand what the phrase "exceeds authorized access" means.

The Seventh Circuit's approach in Citrin can be rejected for this purpose because, as discussed above in relation to the first step in the analysis, it relies on common law agency principles that are irrelevant in the Internet services context. Likewise, the intended use analysis employed by the Fifth and Eleventh circuits (in John and Rodriguez, respectively) is inappropriate because it also presumes a certain relationship between the

---

151 18 USC § 1030(a)(1), (2), (4).
authorizing party and the authorized user. In the Internet services context, however, the user is not expected to understand the provider's interests; such interest could easily be unknown to an everyday user of Internet services. Indeed, because “public website provider[s] can easily spell out explicitly what is forbidden,” there is no reason to infer limitations on an Internet services user’s authorized access solely from the authorizing party’s interests or purpose. As a result, the intended use analysis is unsuitable in the non-employment context because there is no basis in the Internet service context for defining authorization, or its scope, on the understood relationship between an Internet user and authorizer.

Finally, both the Citrin approach and the intended use analysis are suspect—in the CFAA context as a whole—because they are inconsistent with the CFAA’s language. As previously mentioned, the Citrin court’s approach to defining “without authorization” collapses the two-scienter based requirements of the CFAA into one, which is inconsistent with the express language of the CFAA. Furthermore, contrary to the intended use approach adopted by the Fifth and Eleventh circuits, the language of the CFAA conditions liability solely on the type of access used by an individual to acquire data and not on the use of the data acquired. For example, § 1030(a)(2), under which the employee in John was prosecuted, states “[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains [certain types of information] . . . shall be punished.” As the language makes clear, the accessor’s liability under the CFAA only depends on his access to the information being “without authorization,” or “exceeding authorization,” without any regards or mention of the use to which the accessed information is put.

---

152 See notes 72–88 and accompanying text.
153 EF Cultural Travel, 318 F3d at 63.
154 See text accompanying notes 56–60, 148.
155 See generally, 18 USC § 1030.
156 John, 597 F3d at 270.
157 18 USC §1030(a)(2).
C. Void for Vagueness?

Lastly, despite the notable challenges, the void for vagueness doctrine does not operate to completely invalidate the CFAA outside of the employment context. In *Drew*, the court dismissed a CFAA charge on the basis of a Terms of Service violation because, in its view, applying the CFAA to such a broad context would render the Act void for vagueness for the lack of adequate notice to users and the lack of guidance for law enforcement.158 Professor Orin Kerr, who served as co-counsel in the *Drew* case, proposed and supports this outcome.159 In his subsequent article, *Vagueness Challenges to the Computer Fraud and Abuse Act*,160 Professor Kerr argues that courts and attorneys should continue to use the constitutional vagueness doctrine to preclude the applicability of the CFAA to cases, such as *Drew*, involving consumer violations of Terms of Service.161 However, as the rest of this Comment will make clear, the void for vagueness doctrine does not limit the CFAA to the employment context. On the contrary, the CFAA can, in a manner consistent with the void for vagueness doctrine, apply to the Internet service context and, more specifically, to cases such as *Drew*.

First, the Supreme Court's interpretation and application of the void for vagueness doctrine counsels against invalidating the CFAA on such a basis. In the recent decision in *Holder v Humanitarian Law Project*,162 the Supreme Court affirmed that a scienter requirement in a statute can counter allegations that the statute is void because it fails to put the public on notice of what conduct is prohibited.163 In that case, the Court ruled that a criminal statute "requiring knowledge of [a] foreign group's designation as a terrorist organization or the group's commission of terrorist acts" gave sufficient notice to save the

158 See text accompanying notes 128–135.
159 *See Drew*, 259 FRD at 451.
161 Id at 1572–73.
162 130 S Ct 2705 (2010).
163 See id at 2720 ("[T]he knowledge requirement of the statute further reduces any potential for vagueness.["]). See also *Village of Hoffman Estates v Flipside, Hoffman Estates, Inc.*, 455 US 489, 499 (1982) ("[A] scienter requirement may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed.").
statute from invalidation on vagueness grounds.\textsuperscript{164} By analogy, the CFAA's scienter requirements—the criminalization of only \textit{knowing} or \textit{intentional} access that is "without authorization" or that "exceeds authorization"—are sufficient to alleviate the notice deficiency perceived by the court in \textit{Drew} because they adequately put the public on notice that certain misuses of computers are criminalized by the CFAA.\textsuperscript{165}

Second, the Supreme Court has also recognized the need for preserving congressional intent when considering whether statutes should be invalidated for vagueness.\textsuperscript{166} For example, the Court recently reiterated that courts must be cautious before striking an entire criminal statute for impermissible vagueness and must instead "consider whether the statute is amenable to a limiting construction" that restricts criminalization to actions Congress clearly meant to penalize.\textsuperscript{167} If a limiting construction is possible in order to render the statute in question constitutionally precise, courts should opt to apply such limiting principles and preserve the statute rather than invalidate it on vagueness grounds and completely eschew the congressional intent underlying its enactment.\textsuperscript{168} The circuit courts have undertaken precisely this exercise by developing definitions of "without authorization" and "exceeds authorized access." Those

\textsuperscript{164} Humanitarian Law Project, 130 S Ct at 2719–20.

\textsuperscript{165} Although the \textit{Drew} court conceded that scienter requirements can save a statute from vagueness challenges, it concluded that the word \textit{intentionally} in the relevant CFAA provision did not qualify as a scienter requirement because it required only a "conscious violation of a website's Terms of Service." \textit{Drew}, 259 FRD at 467. In so finding, the \textit{Drew} court distinguished prior Ninth Circuit precedent holding that the word \textit{intentionally} in the CFAA satisfied the scienter requirement because the inclusion of that word meant that the CFAA did "not criminalize otherwise innocent conduct . . . [and required] the Government [to] prove that the defendant intentionally accessed a [computer]" in violation of one of the authorization provisions. Id at 467, quoting \textit{United States v Sablan}, 92 F3d 865, 869 (9th Cir 1996). However, in attempting to distinguish that Ninth Circuit precedent, the \textit{Drew} court focused on factual differences between the two cases and failed to explain how the meaning of \textit{intentionally} was fact-specific. See \textit{Drew}, 259 FRD at 467. Thus, the \textit{Drew} court's opinion does not represent strong precedent for holding that \textit{intentionally} is an unsatisfactory scienter requirement. Moreover, the \textit{Drew} court that other portions of the CFAA—including the felony violation of 18 USC § 1030(a)(2)—have adequate scienter requirements. See id at 467 n 31.

\textsuperscript{166} See, for example, \textit{Philbrook v Glodgett}, 421 US 707, 713 (1975) ("Our objective in a case [expounding a statute] is to ascertain the congressional intent and give effect to the legislative will.").

\textsuperscript{167} \textit{Skilling v United States}, 130 S Ct 2896, 2905 (2010).

\textsuperscript{168} Id.
limiting principles can be adapted for and extended to the Internet services context.\textsuperscript{169}

Third, arguments that the CFAA does not sufficiently put the public on notice that criminal liability can arise out of a contractual agreement\textsuperscript{170} are shortsighted and incomplete. While it is true that while the CFAA does not by its actual language condition liability on the violation of a contractual agreement, the CFAA is clear that liability is based on the limits imposed by the authorizing party.\textsuperscript{171} As this Comment and the very language of the CFAA highlight, CFAA liability rests on whether the accesser's conduct "exceeds authorization" or is "without authorization." Correspondingly, liability based on the limits of authorization requires an authorizing party to dictate the terms of authorization. Consistent with CFAA employment context cases, the terms of authorization can properly be communicated and enforced through contractual agreements\textsuperscript{172} even in the Internet service context.

Accordingly, the CFAA is not rendered void for vagueness outside of the employment context for several reasons: its scienter requirements adequately put the public on notice of what computer misuses may violate the CFAA; a limiting construction of the CFAA in the Internet service context can render the statute sufficiently precise to overcome constitutional vagueness challenges; and CFAA liability predicated on a contractual agreement is not inapposite to the language of the statute.

In conclusion, the CFAA is applicable outside of the employment context to the Internet services context consistent with the demarcations underlined in this Part. First, the distinction between "without authorization" and "exceeds authorization" must be coherently upheld as it was in the Ninth Circuit's holding in \textit{Brekka} and \textit{Nosal}.\textsuperscript{173} Second, an accesser's

\textsuperscript{169} For a discussion of possible limiting principles in the non-employment context, see Part V.

\textsuperscript{170} This argument was embraced by the court in \textit{Drew}, which took issue with the fact that the CFAA was not explicit that liability could attach to a contractual relationship. \textit{Drew}, 259 FRD at 464.

\textsuperscript{171} See generally 18 USC §1030 (creating CFAA liability for conduct that "exceeds authorized access" or is "without authorization").

\textsuperscript{172} See, for example, \textit{Citrin}, notes 56–59 and accompanying text, and \textit{John} and \textit{Rodriguez}, notes 78–88 and accompanying text.

\textsuperscript{173} See Part IV.A.
liability under the “exceeds authorization” provision of the CFAA must be defined by reference to the limits of authorization and not to the use for which the accessed information is employed.\textsuperscript{174} Third, in addition to the CFAA’s scienter requirements, limiting principles can preserve the CFAA in the Internet service context and overcome constitutional vagueness challenges.\textsuperscript{175}

V. PROPOSED LIMITS ON THE CFAA IN THE INTERNET SERVICE CONTEXT

As Part IV demonstrated, the CFAA should be interpreted in a manner that maintains an actual difference between the meaning of “exceeding authorization” and “without authorization.” The current circuit split as to the meaning of “exceeding authorization” can also be resolved to shed some clarity on CFAA liability by rejecting intended use analysis and the Seventh’s Circuit application of duty of loyalty principles. Lastly, Part IV argued that if proper limiting principles can be applied to the CFAA, then the CFAA is not void for vagueness in the online consumer context. This Part provides examples of limiting principles that can be imported into the CFAA in the membership-required, online networking context and in other Internet services contexts. Specifically, this Part will propose a number of limitations that can be utilized by courts and prosecutors in the non-employment context.

A. Limiting the Meaning of Access

Outside of the employment context, the term access in the CFAA should not be interpreted in a way that considers the defendant’s use of the access or use of the information obtained through such access. Instead, the term access should be construed to refer to the accessor’s violative breach of a restricting barrier that precedes and enables his obtainment of information. This construction is consistent with both the language of the CFAA and the Ninth Circuit’s approach in\textit{Brekka} and\textit{Nosal},\textsuperscript{176} and it obviates the need for an accessor to understand and advance the authorizer’s objectives.

\textsuperscript{174} See Part IV.B.
\textsuperscript{175} See Part IV.C.
\textsuperscript{176} See notes 99–115 and accompanying text.
In passing the CFAA, Congress was primarily concerned with combatting computer hacking. To effectuate that purpose, Congress chose to criminalize certain access to computers. That is, instead of criminalizing the use of hacked information or the use of hacked access—which it could have done—Congress criminalized the access itself. Yet any understanding of access that considers the use to which such access is put fails to respect that congressional choice. This limitation is particularly relevant in the non-employment context where consumers of Internet services have no reasonable means of discovering the uses of information an authorizer permits or supports, nor have a preexisting relationship with the authorizer from which to glean the norms of authorization.

B. Applying the Limiting Meaning of Access to the “Without Authorization” Context

Because the CFAA’s language focuses on a defendant’s access rather than use to which the defendant puts such access, courts and prosecutors should use the CFAA’s “without authorization” provision in the Internet services context to combat traditional computer hacking—clandestine access to websites or data warehouses that restrict access to authorized users only. For example, a consumer user should be liable for accessing a computer system “without authorization” if he knowingly bypasses a website’s registration system in order access the website’s information, content, or functionality. A consumer user should also be liable for access “without authorization” if he continues to access a computer system after he becomes aware that his authorization has been revoked. This second situation could arise when a consumer user is removed from a social networking site for improper use but his


178 See 18 USC § 1030(a)(1), (2), (4) (referring to accessing a “computer” “without authorization” or “exceeding authorized access”). See also Kristopher Accardi, Comment, Is Violating an Internet Service Providers’ Terms of Service an Example of Computer Fraud and Abuse? An Analytical Look at the Computer Fraud and Abuse Act, Lori Drew’s Conviction and Cyberbullying, 37 W State U L Rev 67, 77 (2009) (explaining that Congress was prompted to enact the CFAA to “protect[] property interests[,] . . . citizens’ privacy[,] and national security”).
access credentials are not immediately deactivated or he impedes their deactivation.\textsuperscript{179}

C. Applying the Limiting Meaning of Access to the "Exceeding Authorized Access" Context

In the "exceeding authorized access" context, the correct interpretation of access implies that consumer users of online networking services should only be liable in two circumstances. The first is hacking outside of the parameters of authorization. Specifically, a consumer user who becomes a registered member of an online networking site but then uses his membership to access portions of the website that he is not meant to access should be liable. For example, one who registers for Facebook and then, while making use of his access to the profiles of others, contravenes barriers to view information on those other profiles that has been deliberately concealed from the public's view, would be liable for exceeding his authorized access to Facebook. To avoid vagueness concerns, the consumer user must be on notice as to what portions of a website he is not meant to access. However, such notice can be implied from the website's use of technical obstacles such as additional password protection for unauthorized areas or can be given via explicit language warning that advancing to a certain area of the website exceeds authorization.

The second type of "exceeding authorized access" liability for consumer users in the online networking service context is when an agreement between the user and the authorizing party clearly delineates the limits of such user's authorization and the user breaches that agreement. This agreement will very likely take the form of a Terms of Service agreement, which should meet certain criteria in order to avoid vagueness concerns. Many of the criteria suggested below draw on concepts already utilized in the clickwrap context—licensing agreements "in which the vendor requires the consumer to click an 'I Accept' icon or click-

\textsuperscript{179} In effect, this was precisely one of the allegations in the Aaron Swartz case. As Orin Kerr described in a recent blog post, Swartz used JSTOR, a password protected database, to download articles. Once his access was blocked, he repeatedly used other methods to circumvent the blocks. Such actions are not "particularly different from . . . quintessential [examples of] access without authorization." Orin Kerr, The Criminal Charges Against Aaron Swartz (Part 1: The Law) (Volokh Conspiracy Jan 14, 2013), online at http://www.volokh.com/2013/01/14/aaron-swartz-charges/ (visited Sept 15, 2013).
check an unchecked box for the agreement to take effect—because clickwrap agreements are similar in function to Terms of Service Agreements and because they are predicated on a similar relationship between vendors-consumers as the relationship between website authorizers-website users. Furthermore, since several courts have already addressed and elucidated the parameters of enforceable clickwrap agreements, it is more likely that applying these parameters to the Terms of Service context will persuade courts to also enforce Terms of Service agreements.

First, these agreements should be obvious and apparent to the user and should require affirmative assent. Unlike in the Drew case, in which the defendant was able to accept the Terms of Service without accessing or viewing them, access-limiting agreements should be presented to the user, in full form, at the time the user accepts the terms. Of course, there is always the concern that even if agreements are prominently displayed and unavoidable by users, consumers will nevertheless ignore them and assent without reading them. This concern is significantly more important in the CFAA context than in the traditional clickwrap context since CFAA violations can result in criminal liability. Nevertheless, it has long been a tenet of criminal law that ignorance of the law is no excuse and where the defendant has the “possibility of knowledge” the law will be enforced.


181 See, for example, Specht v Netscape Communications Corp, 306 F3d 17, 20–21 (2d Cir 2002) (finding that users did not “unambiguously manifest assent” to a licensing agreement when they downloaded free software without knowledge that downloading the software would indicate assent to terms that would not be apparent to a “reasonably prudent Internet user”); Caspi v Microsoft Network LLC, 323 NJ Super 118, 125–26 (1999) (upholding the enforceability of an online agreement that gave users ample opportunity to review before affirmatively assenting to the agreement by clicking an “I Agree” button).

182 See Casamiquela, 17 Berkeley Tech L J at 486 & n 97 (cited in note 180) (explaining that the requirements of enforceable clickwrap is that the agreement be automatically presented to the consumer and that it require the consumer to affirmatively assent to its terms). See also ProCD v Zeidenberg, 86 F3d 1447, 1452 (7th Cir 1996) (emphasizing that the software “splashed the agreement on the screen” so that the consumer could not avoid it).

against him. Additionally, even in the void for vagueness context, at least one Supreme Court justice has affirmed this concept explaining that “[n]o constitutional value is served by permitting persons who have avoided any possibility of attempting to ascertain how they may comply with a law to claim that their studied ignorance demonstrates that the law is impermissibly vague.” Therefore, where users deliberately ignore the terms and assent to agreements that are conspicuously presented for their review, such ignorance should not preclude CFAA liability.

Second, only the portions of these agreements that deal with access restrictions should be enforced via the CFAA. Use restrictions appearing in these agreements should not be enforced under the CFAA’s criminal or civil provisions. This requirement respects the proper interpretation of access discussed above. In addition to disallowing contractual use restrictions in Terms of Service agreements from being enforced through CFAA liability, the CFAA’s requirement that unauthorized or excessive access cause “loss or damage” in order for liability to attach further ensures that website providers are not able to criminalize harmless violations of access limitations. Accordingly, even if a user did exceed his authorized access, he would nevertheless not be liable under the CFAA if his access did not cause “loss or damage.”

Third, the terms of the agreement that give rise to authorized or excessive access charges should not be subject to unilateral modification by the authorizing party without notice to the user. Although a website provider should be permitted to change the terms of a Terms of Service agreement without

---

186 In other words, a Terms of Service provision prohibiting a user from accessing information to which he does not properly have the password to would be enforceable under the CPAA, while a provision prohibiting a user from using information for financial gain would not be enforceable under the CPAA because it would amount to an inappropriate contractual use restriction.
187 See Part V.A.
188 18 USC § 1030(g).
189 See Douglas v United States District Court for the Central District of Cal, 495 F3d 1062, 1066 (9th Cir 2007) (finding that a party cannot unilaterally change the terms of an online contract without the other party’s consent since a “revised contract is merely an offer and does not bind the parties until it is accepted”).
negotiating with the user, the user must be notified of, and
given the option to accept or deny, any changes to terms that
limit authorized access if the website provider wants to be able
to enforce those limits through CFAA liability. This restriction
militates against as-applied vagueness challenges to the CFAA
because previously permissible access will not suddenly be made
criminal without the user’s knowledge.

Fourth, the information from Terms of Service agreements
that pertains to access limitations should be presented to the
user in a prominent manner; for example, with a heading and
colorful highlighting that informs the user that the provision
could potentially give rise to civil or criminal liability.¹⁹⁰ Such a
warning suggests to the user that portion of the agreement
should be read closely.¹⁹¹ Accordingly, void for vagueness
concerns would be further alleviated by this requirement
because adequate notice to the user would be magnified through
the prominence of the text.

These four limitations on the use of Terms of Service
agreements as bases for CFAA liability go a long way towards
meeting the void for vagueness challenges raised against the
CFAA in the Internet services context. Indeed, by using these
limitations to answer the vagueness challenges, courts and
prosecutors can constitutionally extend CFAA liability beyond
the employment context without worrying about invalidation
under the void for vagueness doctrine. This is important because
extending the CFAA to the non-employment context is
consistent with Congress’ purpose in enacting the CFAA: to
address all instances of computer hacking.¹⁹² Additionally,
maintaining the CFAA to impose liability for certain breaches of
access in the Internet service context will make the Internet
safer for all consumers, especially at a time when users are
increasingly placing their private information online.¹⁹³

¹⁹⁰ Juliet M. Moringiello and William L. Reynolds, Survey of the Law of Cyberspace:
that highlighting, bolding, and capitalizing important language would satisfy
conspicuousness requirements and help support the validity of an online contract).

¹⁹¹ Id.

¹⁹² See Part I, notes 20–27 and accompanying text.

¹⁹³ Chris Rose, The Security Implications of Ubiquitous Social Media, 15 Intl J of
Management & Information Systems 35, 37 (2011) (describing an increase in “over-
sharing whereby people disclose too much information”).
If these changes are incorporated into the current Terms of Service regime, there could potentially be a chilling effect on consumers' use of websites requiring registration. However, because consumers in the Internet context quickly adapt to changing norms, any such chilling effect will likely be temporary. In addition, because the portions of Terms of Service agreements dealing with CFAA liability are likely to be substantially similar across websites, consumers will quickly become accustomed to such terms, further ensuring that any such chilling effect is only temporary. Lastly, a minor chilling effect might even be desirable when weighed against the activities that CFAA liability in the Internet services context will deter.

VI. CONCLUSION

The CFAA was enacted to combat computer hacking at a time when personal computers were scarce, little was known about the potential of hacking, and the Internet was in its infancy. Since then, much of the expounding of the CFAA has taken place in the employment context and uncertainty about its exact meaning persists. This obscurity is especially evident in the continuing conflict between the application of "without authorization" and "exceeding authorization," as well as the ongoing struggle to define "exceeding authorization."

Against this dissonant backdrop, the added challenge of the increased prevalence of Internet services and online networking websites that often dictate consumers' assent to complex Terms of Service agreements, fortifies the uncertainty of the CFAA. Nevertheless, the approaches used by courts in applying the CFAA to the employment context are often unavailing in the Internet service context. Additionally, recent cases such as Drew and Aaron Swartz's prosecution evince that there are conflicting

---

194 See id (noting that increased comfort with using the Internet has led many consumers to conform to new norms, going from reluctance to even disclose one's name on the Internet to comfort that often leads users to over-share information).

195 If the limitations on Terms of Service agreements suggested in this Comment, and others, are adopted by website providers and used as bases for CFAA liability, their enforceability in the CFAA context will eventually be litigated. As litigation highlights language that makes Terms of Service agreements enforceable under the CFAA, website providers will strive to use that exact language because of the assurance that such language will allow them to bring successful suits for CFAA violations. Accordingly, there will be a significant amount of uniformity among different website providers.
conceptions of the applicability of the CFAA to the Internet service context: both a desire to apply the CFAA and to challenge its applicability outside of the employment context.

Despite these complications, maintaining the CFAA and determining its applicability to the Internet service context is central to maintaining the congressional intent that underscored the passage of the CFAA and making Internet user safer for all consumers. This Comment emphasizes the applicability of the CFAA to the Internet service context by embracing a coherent distinction between "without authorization" and "exceeding authorization" based on whether the user has any access privileges to the computer or information network in question. Furthermore, it incorporates a definition of "exceeding authorization" that gives no regard to the use to which improperly accessed information is put, and focuses instead on the practical limitations to access as expressed through technical blocks and contractual agreements between website providers and website users. Lastly, this Comment proposes limitations to the types of agreements between consumers and website providers that will support the imposition of CFAA liability to ensure that the Act will withstand constitutional void for vagueness challenges even when applied to Terms of Service violations, as it was in the Drew case. Together, these approaches suggest a comprehensive approach to holding Internet users responsible for CFAA violations in the Internet service context.