INTERPRETING THE COMPUTER FRAUD AND ABUSE ACT

By Lee Goldman*

Volume XIII – Fall 2012

I. INTRODUCTION

Computers play an integral role in today's society. They do everything from maintaining payroll accounts and issuing checks to providing unlimited access to information worldwide. While computers provide many benefits, they are increasingly used as tools for wrongdoing, causing estimated losses of billions of dollars each year.[1] Computer hackers can, among other things, fraudulently alter accounts, steal business or personal information, and corrupt or disable computer systems. Congress enacted and has repeatedly amended the Computer Fraud and Abuse Act ("CFAA") to combat the increasing proliferation of computer crimes.[2]

The primary substantive provisions of the CFAA are predicated on the defendant accessing a protected computer without authorization or by exceeding authorized access.[3] A majority of the Circuit Courts of Appeals, to address the meanings of "without authorization" or "exceeded authorized access," has adopted definitions that alarmingly broaden the scope of the Act.[4] For example, if a child accesses a text message from a parent's phone without permission, she is subject to criminal prosecution. Similarly, under the Circuit Courts of Appeals' majority approach to determining the scope of the phrase "exceeds authorized access," a person misstating

* Professor of Law at the University of Detroit-Mercy; J.D., 1979, Stanford University.

[1] *See* Shawn E. Tuma, "*What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S. C. L. REV. 141, 150 (2011); Orin S. Kerr, *Cybercrime's Scope: Interpreting Access and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1605 (2003); Charlotte Decker, Note, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 961 (2008); *see also* Tuma, *supra*, at 146, 151 (citing studies indicating that 65% of people worldwide have been the victim of some type of cyber crime and 80-90% of businesses have experienced information security breaches).

[2] *See* 18 U.S.C. §1030 (2006 & Supp. II 2008); *see also infra* notes 7-18 and accompanying text.

[3] *See infra* notes 15-18 and accompanying text.

[4] *See infra* notes 19-50 and accompanying text.

their age on a dating website could be subject to imprisonment. These results are untenable. Two recent Circuit Courts of Appeals decisions have adopted narrower definitions of the phrases "without authorization" and "exceeded authorized access."[5] While these definitions represent an improvement over the broader tests, the narrower definitions are incomplete and may exclude paradigm cases of computer fraud.[6] Accordingly, this article argues that the Courts of Appeals have not adequately interpreted the foundational terms of the Act and recommends an interpretation of the Act that builds upon the narrower definitions to comprehensively define the scope of the Act's coverage.

Part II of this article will provide a brief description of the CFAA. Part III will describe the three primary approaches that the courts have adopted to define "without authorization" and "exceeds authorized access." Part IV will discuss the shortcomings of each of the three primary approaches. Part V will provide a preferred interpretation of the Act, suggest possible amendments to the Act to ensure that courts follow the recommended interpretation, discuss the benefits of following this article's recommendations, and illustrate the application of the suggested approach.

II. A BRIEF DESCRIPTION OF THE CFAA

The CFAA was enacted in 1984 as a limited criminal statute to punish persons both misusing computers to obtain national security secrets or personal financial records and hacking into government computers.[7] Through a series of amendments, the scope of the Act has greatly

[5] *See* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).
[6] *See infra* notes 148-54 and accompanying text.
[7] *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1994); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564 (2010).

expanded.[8] Whereas the Act originally applied to misuse of computers used by financial institutions or the United States government, the current version covers all computers used in or affecting commerce, including computers located outside the United States that affect commerce or communication in the United States.[9] Given access to the Internet, this covers virtually all business, home and laptop computers.[10]

The 1994 Amendments to the Act provided for civil liability as well.[11] Under subsection (g) of the current Act, "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."[12] However, a private plaintiff is limited to economic damages and generally, must show a loss[13] aggregating at least $5,000 in value.[14]

New substantive provisions also have been added to the Act. The three most significant provisions, sections 1030(a)(2)(C), (a)(4) and (a)(5), cover obtaining computer information without authorized access, certain computer frauds, and some actions resulting in damage or

[8] *See* Kerr, *supra* note 1, at 1563-71 (providing a detailed description of each of the amendments to the CFAA).
[9] *See* 18 U.S.C. § 1030(e)(2)(B) (2006 & Supp. II 2008).
[10] *See* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007); United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009), *citing* Reno v. ACLU, 521 U.S. 844, 849 (1997); *see also* Kerr, *supra* note 1, at 1663. The Act's definition of "computer" extends beyond coverage of traditional computers. "Computer" is defined to include any device that is "an electronic … or other high speed data processing device performing logical, arithmetic, or storage functions…." Under this definition cell phones, iPods, computerized airbags and a myriad of other electronic devices are computers. *See* United States v. Kramer, 631 F.3d 900, 902-3 (8th Cir. 2011); United States v. Mitra, 405 F.3d 492, 495-96 (7th Cir. 2005); Kerr, *supra* note 7, at 1577.
[11] *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796; Dice Corp. v. Bold Technologies, No. 11-13578, 2012 WL 263031, at *5 (E.D. Mich. Jan. 30, 2012).
[12] 18 U.S.C. § 1030(g) (2006 & Supp. II 2008).
[13] "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11) (2006 & Supp. II 2008). Courts have held that "loss" "encompasses only two types of harm: costs to investigate and respond to an offense, and costs incurred because of a service interruption." Alliantgroup, L.P. v. Feingold, 803 F. Supp. 2d 610, 630 (S.D. Tex. 2011).
[14] *See* 18 U.S.C. § 1030(g) (2006 & Supp. II 2008). A loss of $5,000 is required unless the plaintiff can show an effect on the medical examination, diagnosis, treatment, or care of an individual, physical injury to any person, a threat to public health or safety or damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security. *See* 18 U.S.C. §§ 1030(c)(4)(A)(I)-(V) (2006 & Supp. II 2008). Very few plaintiffs allege any of these alternatives to a loss of $5,000. *See* Tuma, *supra* note 1, at 183.

loss to a protected computer, respectively.[15] More specifically, subsection (a)(2)(C) imposes liability on a person who, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains …information from any protected computer."[16]

Section (a)(4) prohibits use by any person who,

> 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.[17]

Finally, section (a)(5) provides for punishment of any person who,

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[18]

Violations under sections (a)(2) and (a)(4) require that the person accessing the protected computer is "without authorization" or "exceeds authorized access. Section (a)(5) imposes liability for unintentional damage or loss only where the access is "without authorization." Accordingly, the interpretation of the terms "without authorization" and "in excess of authorization" is critical in understanding the scope of the CFAA.

---

[15] 18 U.S.C. § 1030(a) (2006 & Supp. II 2008). Amendments to the Act also prohibit trafficking, with an intent to defraud, "in any password or other information through which a computer may be accessed without authorization…", and extorting money or other thing of value through threats to cause damage to a protected computer or threats to obtain or impair the confidentiality of information. 18 U.S.C. § 1030 (a)(6)-(7).

[16] 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. II 2008).

[17] 18 U.S.C. § 1030(a)(4) (2006 & Supp. II 2008).

[18] 18 U.S.C. § 1030(a)(5) (2006 & Supp. II 2008). Fraud under this section simply requires wrongdoing, not the elements of common law fraud. *See, e.g.*, T-Mobile USA, Inc. v. Terry, No. 3:11-cv-5655-RBL, 2012 WL 1409287, at *6 n.1 (W.D. Wash. Apr. 23, 2012); eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009); Shurguard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000). Allegations of fraud under this section also do not need to meet the specificity requirements for fraud under Rule 9(b) of the Federal Rules of Civil Procedure. *See* Facebook, Inc. v. MaxBounty, Inc. 274 F.R.D. 279, 284 (N.D. Cal. 2011); SKF USA, Inc. v. Bjerkness, 636 F. Supp. 2d 696, 719 n.13 (N.D. Ill. 2009).

III. THE EXISTING APPROACHES FOR DEFINING "WITHOUT AUTHORIZATION" AND "EXCEEDING AUTHORIZED ACCESS"

Courts have not agreed on the proper interpretation of "without authorization" and "exceeds authorized access." Rather, they have adopted three different approaches to interpreting these terms. Each of these approaches is described below.

A. Agency Approach

The agency approach arose in the employer-employee relationship context and took a broad view of who is unauthorized to access a computer, thereby expanding the potential scope of the CFAA. This approach originated in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*,[19] and gained credibility following Judge Posner's adoption of the approach in *International Airport Centers, L.L.C. v. Citrin.*[20]

In *Shurgard*, the plaintiff alleged that former employees appropriated trade secrets stored on the plaintiff's computer in violation of sections 1030(a)(2)(C), (a)(4), and (a)(5)(C).[21] The defendant moved to dismiss for failure to state a claim arguing that the foundation for a violation of those sections, access without authorization or exceeding authorized access, was not alleged and could not be proven.[22] The Court denied the defendant's motion, reasoning that under the Restatement (Second) of Agency, the employees' authorization ended when they obtained information on behalf of their employer's competitor.[23] Quoting the Restatement, the Court stated,

[19] *Shurgard Storage Ctrs.*, 119 F. Supp. 2d 1121.
[20] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).
[21] *Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1122-23. The plaintiff also alleged a variety of state claims. *Id.* at 1122.
[22] *Id.* at 1124.
[23] *Id.* at 1125.

> Unless 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.[24]

In *Citrin*, the defendant deleted all of the data from his company laptop after he decided to leave the plaintiff's employ and go into business for himself. Judge Posner, citing *Shurgard* and the Restatement, held that the authorization to access the computer terminated when the defendant "resolved to destroy files that . . . were also the property of the employer, in violation of the duty of loyalty that agency imposes on an employee."[25]

Especially with Justice Posner's imprimatur, many courts have felt compelled to discuss the agency theory for defining "without authorization."[26] However, no other Circuit Court of Appeals has adopted the agency approach. Nonetheless, the agency approach remains the law in the Seventh Circuit[27] and has been followed by a few district courts outside the Seventh Circuit.[28]

B. Contract Approach

The contract approach to defining "without authorization" and "exceeds authorized access" focuses on how the parties agreed to define their rights and duties. Under this approach,

---

[24] *Id.* (*citing* RESTATEMENT (SECOND) OF AGENCY § 112 (1958)). The Court also found support for its decision in ambiguous language from the legislative history of the Act. *Id.* at 1128-29.
[25] *Int'l Airport Ctrs.*, 440 F.3d at 420.
[26] *See, e.g.*, LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009); Farmers Bank & Trust, N.A. v. Witthuhn, No. 11-2011-JAR, 2011 WL 4857926, at *4 (D. Kan. Oct. 13, 2011); Lewis-Burke Assoc., Inc. v. Widder, 725 F. Supp. 2d 187, 192 (D.D.C. 2010); Grant Mfg. & Alloying, Inc. v. McIlvain, No. 10-1029, 2011 WL 4467767, at *6 (E.D. Pa. Sept. 23, 2011); WEC Carolina Energy Solutions, LLC v. Miller, No. 10-cv-2775-CMC, 2011 WL 379458, at *3 n.5 (D.S.C. Feb. 3, 2011); Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010); Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d. 1267, 1272 (M.D. Ala. 2010); US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1192 (D. Kan. 2009); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933 (W.D. Tenn. 2008).
[27] *See, e.g.*, Jarosch v. American Family Mut. Ins. Co., 837 F. Supp. 2d 980, 1021 (E.D. Wisc. 2011).
[28] *See, e.g.*, Am. Family Mut. Ins. Co. v. Hollander, NO. C 08-1039, 2010 WL 2851639, at *2 (N.D. Iowa Jul 20, 2010); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009); NCMIC Finance Corp. v. Artino 638 F. Supp. 2d 1042, 1057-58 (S.D. Iowa 2009); Ervin & Smith Adver & Pub. Relations, Inc. v. Ervin, No. 8:08CV459, 2009 WL 249998, at *8 (D. Neb. Feb. 3, 2009).

the terms of use of a website, the provisions in an employment contract or the terms of other contractual arrangements, allow the parties to define the scope of permission to access any protected computer. If the person who is granted access under the contract violates any of its terms, she is viewed as unauthorized or exceeding authorized access for purposes of the CFAA. The theory behind the contract approach is simple: if a person needs authorization to access a computer, the owner of the computer should be able to restrict or condition the access.[29] When the person obtains information in violation of the restriction or condition, they have exceeded authorization and obtained information they were "not entitled so to obtain."[30]

The First Circuit in *EF Cultural Travel BV v. Explorica, Inc.*,[31] was the first Court of Appeals to adopt the contract approach. In *EF Cultural*, the plaintiff sued a competing tour company and some of the plaintiff's former executives.[32] The plaintiff alleged that the former executives utilized confidential tour codes to enable its competitor to obtain the plaintiff's pricing information with a scraper program.[33] The Court found that the use of this proprietary information violated the plaintiff's broad confidentiality agreement, which prohibited the disclosure of information "'which reasonably might be construed to be contrary to the interests of EF.'"[34] Therefore, the Court concluded that if the plaintiff's allegations were true, the defendants had exceeded the contractually authorized access.[35]

[29] *See, e.g.*, Cont'l Group, Inc. v. KW Prop. Mgmt, LLC, 622 F. Supp. 2d 1357, 1372 (S.D. Fla. 2009).
[30] 18 U.S.C. § 1030 (e)(6) (2006 & Supp. II 2008); *see also* Reply Brief of the Plaintiff-Appellant at 5, United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (No. 10-10038), 2010 WL 6191782.
[31] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).
[32] *Id.* at 579-80.
[33] *Id.* at 579 (describing the use of a scraper program which focused solely on EF's website; a scraper program, like a robot, performs searching, copying and retrieving functions on the web, executing thousands of commands per minute, far in excess of what an individual can do). *See also* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1060-61 (N.D. Cal. 2000); Christine Galbraith, *Access Denied, Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 332-33 (2004).
[34] *EF Cultural Travel BV*, 274 F.3d at 583.
[35] *Id.*

In *U.S. v. Rodriguez*,[36] an employee of the Social Security Administration accessed, for non-business reasons, personal information of several women he knew.[37] The Administration specifically prohibited accessing information from its databases for non-business related purposes.[38] Accordingly, the Eleventh Circuit concluded that "the plain language of the Act forecloses any argument that Rodriguez did not exceed his authorized access."[39]

In *U.S. v. John*,[40] the Fifth Circuit also relied, in part, on contractual limitations on authorization, to support a finding that the defendant exceeded authorized access to information in violation of 18 U.S.C. § 1030(a)(2). In this case, the defendant provided her half-brother with customer account information that enabled him and others to create fraudulent charges.[41] Even though the defendant, as an account manager, was authorized to access customer account information,[42] the Court emphasized that John's use of that information to perpetuate a fraud was contrary to the plaintiff's official policies and therefore, her access for those purposes was "in excess of authorization."[43]

EF Cultural, *Rodriguez*, and *John*, all arose in the employer-employee context. However, several courts have indicated that the contract approach applies outside that milieu. [44] In particular, the contract approach can also be used to deem access in excess of authorization when a website user violates a site's terms of use.[45] For example, in *America Online, Inc. v. LCGM,*

[36] United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010), *cert. denied*, 131 S. Ct. 2166 (2011).
[37] *Id.* at 1260-61.
[38] *Id.* at 1260.
[39] *Id.* at 1263.
[40] United States v. Long, 597 F.3d 263 (5th Cir. 2010).
[41] *Id.* at 269.
[42] *Id.*
[43] *Id.* at 272-73.
[44] *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003); FXDirectDealer, LLC v. Abadi, No. 12 Civ 1796(CM), 2012 WL 1155139, at *6 (S.D.N.Y. Apr. 5, 2012); United States v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998).
[45] *Id.*

Inc.,[46] the Court found that the defendant's use of AOL to send bulk e-mails in violation of AOL's terms of use constituted access in excess of authorization.[47]

A majority of the Circuit Courts of Appeals that have addressed this issue have adopted the contract approach for defining "in excess of authorization."[48] It is also the approach advocated by the Justice Department,[49] and some district court decisions outside those circuits.[50]

C. Plain Meaning Approach

The "plain meaning" approach interprets "without authorization," an undefined term under the Act, as referring to "outsiders"[51] – those without any permission to access the protected computer.[52] This approach construes "exceeds authorized access" as when "insiders," those permitted to access a protected computer, access information on the protected computer that the insider is not so entitled to obtain.[53]

---

[46] *Am. Online*, 46 F. Supp. 2d 444.
[47] *Id.* at 451.
[48] *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001).
[49] Brief for the United States, United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (No. 10-10038), 2010 WL 6191778.
[50] *See, e.g.*, FXDirectDealer, LLC v. Abadi, No. 12 Civ. 1796, 2012 WL 1155139, at *6 (S.D.N.Y. Apr. 5, 2012); Grant Manuf. & Alloying, Inc. v. McIlvain, Civil Action No. 10-1029, 2011 WL 4467767, at *7 (E.D. Pa. Sept. 23, 2011); Cont'l Grp., Inc. v. KW Prop. Mgm't, LLC, 622 F. Supp. 2d 1357, 1372 (S.D. Fla. 2009).
[51] *See* United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007).
[52] *See infra* notes 57-58 and accompanying text.
[53] *See infra* note 59. A few commentators, *see* Garrett D. Urban, Note, *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, 1379-82 (2011); Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 826 (2009), have suggested that courts adopting the plain language approach were really applying the "code-based" approach advocated by Professor Orin S. Kerr in his seminal article, *Cybercrime's Scope: Interpreting Access and "Authorization" in Computer Misuse Statutes*, *supra* note 1. The difference between the two approaches is that the code-based approach presumes that an insider is entitled to obtain all information that is not password (or otherwise technologically) protected. Under the plain language approach, password protected information is just one category of information that an insider is not entitled to obtain. For example, assume a doctor has a password to access all patient files at a hospital. If the doctor uses the password to access files of persons who are not his patients, there could be a violation of section (a)(2)(C) under the plain language approach. There would be no violation under the code-based approach. Only one district court and one lower court state case has explicitly adopted the code-based approach. *See* Facebook, Inc. v. Power Ventures, Inc., No. C 08–05780 JW, 2012 WL 542586, at *1038-*1040 (N.D. Cal. Feb. 16, 2012); State v. Riley, 988 A.2d 1252, 1258 (N.J. Super. 2009).

The Ninth Circuit first adopted the "plain meaning" approach in *LVRC Holdings, LLC v. Brekka*.[54] In that case, an employer brought suit against a former employee alleging, among other things, that the employee e-mailed a number of documents to his personal email account during discussions pertaining to the possibility of purchasing an ownership interest in the plaintiff-company.[55] The Ninth Circuit affirmed summary judgment for the defendant on the plaintiff's CFAA claim, finding that the defendant's access was authorized and that he did not exceed his authorized access.[56] In interpreting the phrase "without authorization," the Court began with the "'fundamental canon of statutory construction … that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.'"[57] Finding the dictionary definition of authorization to be "permission," the Court concluded that the defendant was not "without authorization" because the defendant had permission to access the plaintiff's computer.[58] The Court, referring to the statutory definition in 18 U.S.C. § 1030(e)(6), interpreted "exceeds authorized access" as when "a person has permission to access the computer, but accesses information on the computer that the person is not entitled to access."[59] Given that the defendant was entitled to access the information he e-mailed to his personal account, he could not be found to have exceeded authorized access.[60] The Court specifically rejected the plaintiff's *Citrin*-based argument that permission terminated when the defendant took actions inconsistent with the plaintiff's interest. The Court found the agency approach to be inconsistent with the plain language of the statute and contrary to the rule of lenity.[61]

---

[54] LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).
[55] *Id.* at 1129-30.
[56] *Id.* at 1135.
[57] *Id.* at 1132, *citing* Perrin v. United States, 444 U.S. 37, 42 (1979).
[58] *Id.* at 1133.
[59] *Brekka*, 581 F.3d at 1133.
[60] *Id.* at 1135.
[61] *Id.* at 1134-35. The rule of lenity "requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government." *Id.* at 1135 (quoting United States v. Romm, 455 F.3d

The Ninth Circuit, in an *en banc* decision, recently reaffirmed their decision in *Brekka*, and explicitly rejected the contract approach to defining "exceeding authorized access."[62] In *Nosal*, several employees of an executive search firm downloaded and transferred confidential files to the defendant, a former employee of the search firm, who was starting a competing business.[63] The government acknowledged that the employees had authorization to access the information, but alleged that their actions violated the plaintiff's policy of forbidding the disclosure of confidential information.[64] To support its position, the government focused on the word "so" in section 1030(e)(6) ("accesser is not entitled *so* to obtain or alter" (emphasis added)). The government argued that "so" meant "in that manner," which it claimed had to refer to restrictions on information use.[65] A narrower reading, the government argued, would make the word "so" superfluous.[66] The original Court of Appeals panel adopted the government's argument.[67]

Although the *en banc* panel acknowledged that the government's contract approach-based argument, with its reliance on the word "so," was not an unreasonable reading of the statute,[68] it reversed the three-judge panel's decision, believing that the government's reading would unduly expand the scope of the Act.[69] The Court reasoned that "the government's interpretation would transform the CFAA from an anti-hacking statute into an expansive

---

990, 1001 (9th Cir. 2006)). The rule "vindicates the fundamental principle that no citizen should be held accountable for violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed." *Id.* at 1134-35(quoting United States v. Santos, 553 U.S. 507, 514 (2008)). The *Brekka* court reasoned, "If the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA." *Id.* at 1135.

[62] *See* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

[63] *Id.* at 856.

[64] *Id.*

[65] *Id.* at 857.

[66] *Id.*

[67] *See* United States v. Nosal, 642 F.3d 781 (9th Cir. 2011), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012).

[68] *Nosal*, 676 F.3d at 858.

[69] *Id.*

misappropriation statute."[70] The Court was unwilling to displace a substantial portion of the common law absent clear Congressional intent to do so.[71] The Court also feared that the government's position would criminalize "minor dalliances" by people unaware that their conduct violated any criminal prohibition.[72] For example, employees routinely use work computers for personal reasons, yet many corporate policies prohibit such uses.[73] The possibility of liability for violation of a website's terms of use was even more troubling to the court.[74] The Court cited Google's policy, since changed, forbidding minors from using its services.[75] Under the government's approach, a seventeen year-old, who researched a school paper on Google, would have violated section (a)(2)(C) of the Act. Such results were particularly troubling to the Court given the low number of people who actually read or understand the companies' terms of use.[76] Finally, the Court denied that its interpretation would make the word "so" in section 1030(e)(6) superfluous:

> The word has meaning even if it doesn't refer to use restrictions. Suppose an employer keeps certain information in a separate database that can be viewed on a computer screen, but not copied or downloaded. If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not "entitled *so* to obtain." Or, let's say an employee is given full access to the information, provided he logs in with his username and password. In an effort to cover his tracks, he uses another employee's login to copy information from the database. Once again, this would be an employee who is authorized to access the information but does so in a manner he was not authorized "so to obtain." Of course, this all assumes that "so" must have a substantive meaning to make sense of the statute. But Congress could just as well have included "so" as a connector or for emphasis.[77]

[70] *Id.* at 857.
[71] *Id.*, *citing* Jones v. United States, 529 U.S. 848, 858 (2000).
[72] *Id.* at 859.
[73] *Nosal*, 676 F.3d at 860
[74] *Id.* at 860-61.
[75] *Id.* at 861.
[76] *Id.* at 862.
[77] *Id.* at 858.

Most recently, the Fourth Circuit followed the Ninth Circuit's basic approach but interpreted the Act even more narrowly than the approach suggested by the court in *Nosal*.[78] In *WEC Carolina Energy Solutions LLC,* an employee with access to confidential information downloaded that information to his personal computer in violation of the company policy, which prohibited such downloads.[79] After he resigned from his position with the plaintiff, the defendant used that information to solicit an account for plaintiff's competitor.[80] The Fourth Circuit, citing the Ninth Circuit's decisions in *Nosal* and *Brekka,* and relying on the rule of lenity and the plain language of the Act, held that the defendant's actions did not violate the Act.[81] The Fourth Circuit interpreted the word "so" as a connector or a term of emphasis, and specifically rejected the Ninth Circuit's suggested alternative meanings of the word.[82] The court stated, "Congress has not clearly criminalized obtaining or altering information 'in a manner' that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter."[83]

To date, the Ninth and Fourth Circuits are the only Courts of Appeals to adopt the plain meaning approach.[84] However, a majority of the recent district court decisions that are not bound by opposing precedent have followed the Ninth Circuit approach.[85] Some of those courts,

---

[78] *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).
[79] *Id.* at 202.
[80] *Id.*
[81] *Id.* at 207.
[82] *Id.*
[83] *Id.* at 206.
[84] *See WEC Carolina Energy Solutions,* 687 F.3d at 206*; Nosal*, 676 F.3d 854; *Brekka*, 581 F.3d 1127.
[85] *See* Farmers Bank & Trust, N.A. v. Witthuhn, No. 11-2011- JAR, 2011 WL 4857926, at *4 (D. Kan. Oct. 13, 2011) ("the *Brekka* line of cases … has recently gained critical mass"); Lewis-Burke Assoc., LLC v. Widder, 725 F. Supp. 2d 187, 192-93 (D.D.C. 2010) (same); *see also* Ajuba Int'l, LLC v. Saharia, No. 11–12936, 2012 WL 1672713, at *10-11 (E.D. Mich. May 14, 2012); Grant Mfg. & Alloying, Inc. v. McIlvain, No. 10–1029, 2011 WL 4467767, at *6 (E.D. Pa. Sept. 23, 2011); United States v. Aleynikov, 737 F. Supp. 2d 173, 192 (S.D.N.Y. 2010); Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 383-84 (S.D.N.Y. 2010); Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d. 1267, 1272 (M.D. Ala. 2010); ReMedPar, Inc. v. AllParts Medical, LLC, 683 F. Supp. 2d 605, 612-13 (M.D. Tenn. 2010); US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1192-93 (D. Kan. 2009); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 935-36 (W.D. Tenn.

however, have indicated that they would use a hybrid approach to define "in excess of authorization,"[86] suggesting that the "plain language" is not so plain. That is, they would consider contractual limitations when deciding whether a defendant was entitled to obtain or alter information on the protected computer.[87]

The plain language approach is an incomplete solution for defining "without authorization" and "exceeding authorized access" under the Act and may exclude paradigm cases of computer fraud. However, it is a better approach than the agency and contract approaches, both of which, improperly and unnecessarily expand the scope of the Act to cover employee breach of loyalty or theft of trade secret cases.

IV. THE SHORTCOMING OF THE EXISTING APPROACHES FOR DEFINING "WITHOUT AUTHORIZATION" AND "EXCEEDING AUTHORIZED ACCESS"

A. Agency Approach

The agency approach is the most inconsistent approach with the language and the legislative history of the Act. It also has the greatest potential to produce absurd results. The apparent motivation for adopting the agency approach is to punish theft of trade secrets. However, it is neither necessary nor desirable to contort the Act to achieve that result.

As the Court indicated in *Brekka*, no language in the CFAA supports the "argument that authorization to use a computer ceases when an employee resolves to use the computer contrary

---

2008). Many of these courts, much like the Court in *Brekka*, explain that 1) the plain language of the Act prohibits improper access, not misuse or misappropriation, 2) the rule of lenity requires interpreting the Act narrowly and 3) the legislative history of the Act indicates the purpose was to prevent hacking, not misappropriation. *See, e.g.*, *Ajuba*, 2012 WL 1672713, at *11; *Grant Mfg. & Alloying*, 2011 WL 4467767, at *7. *University Sports Pub. Co.*, 725 F. Supp. 2d at 383-84; *US Bioservices Corp.*, 595 F. Supp. 2d at 1193-94; Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *3-4 (E.D. Pa. 2007).

[86] *See* Farmers Bank & Trust, N.A. v. Witthuhn, 11-20110 JAR, 2011 WL 4857926, at *4-*5; Grant Mfg. & Alloying, Inc. v. McIlvain, No. 10-1029, 2011 WL 4467767, at *7.

[87] *See also*, Pamela Taylor, Comment, *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, 230-31 (2012) (recommending adoption of the *Brekka* "narrow view" and suggesting employers can protect themselves through company policies on access).

to the employer's interest."[88] Rather the "plain language" (to the extent language is ever "plain") is to the contrary. The CFAA prohibits "unauthorized access" to information; it does not prohibit the misuse or misappropriation of information.[89] The statutory definitions of damage and loss also suggest that the Act is concerned with computer hacking, alteration of data or information, and disruption of computer services; it is not concerned with the misuse of information, injury to one's competitive position, or loss of revenue. Damage is defined as "any impairment to the integrity or availability of data, a program, a system or information."[90] Loss is "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any consequential damages incurred because of interruption of services."[91] Finally, the agency approach conflates "unauthorized access" with "exceeds authorized access" in employee-employer cases, the only context in which the agency theory is applicable. That is, an employee who exceeds authorized access has breached her duty of loyalty and therefore, she would be unauthorized under the agency theory.

One court has suggested that the agency approach "does not focus on an employee's later misuse of information but instead, it focuses on an employee's initial *access* to the employer's computer with the intent to either obtain information or defraud the employer."[92] This view is problematic on several levels. First, stating that the focus is on access and not misuse seems disingenuous when the intent at the time of access can only be proven by subsequent misuse. Second, an employee's *initial* access will rarely be a breach of their duty of loyalty. Rather,

[88] LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).
[89] *See* Orbit One Commc'n, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008); Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499-09 (D. Md. 2005).
[90] 18 U.S.C. § 1030(e)(8) (2006 & Supp. II 2008).
[91] 18 U.S.C. § 1030(e)(11) (2006 & Supp. II 2008).
[92] NCMIC Finance Corp. v. Artino, 638 F. Supp. 2d 1042, 1059 (S.D. Iowa 2009).

employees will typically breach their duty of loyalty during a workday in which initial access to the computer was for proper work purposes. Third, the court's approach would treat similar situations disparately without any justification. For example, suppose an employee emails confidential information to her personal computer so that she can use it for work-related purposes at home. If that employee later sent confidential information to her employer's competitor from home, there would be no violation of the Act because she is authorized to use her own computer and the information was "obtained" from the "protected computer" with authorization. To suggest that such an employee should be treated differently than the employee who sends the same information from their work computer is anomalous. Fourth, a focus on intent at the time of access is troublingly subjective. It also makes much of the language in section (a)(4) of the Act superfluous in employee-employer cases. That section requires "intent to defraud."[93] Yet if there was intent to defraud, which is obviously contrary to the employer's interests, there would automatically be no authorization, making the "without authorization" or "exceeds authorized access" requirement superfluous.[94]

Although the statutory language is the best indicator of Congressional intent, the legislative history of the Act also suggests that Congress did not wish to define "without authorization" by the agency approach. According to the legislative history, the Act was principally designed to cover "hackers" and punish offenses consummated on a computer.[95]

[93] 18 U.S.C. § 1030(a)(4) (2006 & Supp. II 2008).

[94] A standard canon of statutory interpretation is, "a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous." *See* Regions Hosp. v. Shalala, 522 U.S. 448, 467 (1998).

[95] *See* 132 CONG. REC. H3275-04, 1986 WL 779755 (statement of Rep. Hughes) ("[C]omputer technology-with all its gains-has left us with a new breed of criminal: The technologically sophisticated criminal who breaks into computerized data files. One element of this expanding group of electronic trespassers-the so-called hacker…."); *Id.* (statement of Rep. Nelson) ("[W]e are confronting a new type of criminal today. It is not the kind of criminal who uses the crowbar, but a criminal who uses the computer keyboard …"); S. Rep. 99-432, at 9, 99th Cong. 2d Sess. 1986, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487 (1986) (Section 1030(a)(4) requires "a showing that the use of the computer or computers in question was integral to the intended fraud and was not merely incidental.").

Nevertheless, the agency approach is designed to cover misappropriation cases, cases in which the "locus of wrongful conduct" is not the computer.[96] The computer is "merely the fortuitous place" where information was obtained.[97] Misappropriation is consummated by disclosing information to a competitor regardless of whether the information is obtained on a computer or from the employer's files or wastebasket.[98]

Application of the agency approach would also federally criminalize theft of trade secrets without all the requirements of traditional trade secret law. Misappropriation of information is not actionable under the Uniform Trade Secrets Act unless the information derives independent economic value from not being generally known and the plaintiff uses reasonable efforts to maintain its confidentiality.[99] On the other hand, misappropriation of information can be actionable under the agency approach pursuant to section 1030(a)(2)(C) without satisfying either requirement.[100] It is doubtful that Congress wished to displace a substantial portion of the common law without clearly conveying that intent.[101] To the contrary, the Economic Espionage Act of 1996[102] evidences Congress' desire to maintain the traditional requirements of trade secret protection. That Act criminalizes theft of trade secrets,[103] and includes in its definition of "trade secret" the same requirements contained in the Uniform Trade Secrets Act.[104]

The agency approach also has the potential to produce absurd results that could not have been intended by Congress. For example, an employee might be criminally liable for checking

[96] *See US Bioservices Corp.*, 595 F. Supp. 2d at 1194; Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007).
[97] *Brett Senior & Assocs.*, No. 06-1412, 2007 WL 2043377, at *4.
[98] *See U.S. Bioservices Corp.*, 595 F. Supp. 2d at 1194; *Brett Senior & Assocs.*, 2007 WL 2043377, at *4 n.7.
[99] *See* Uniform Trade Secrets Act § 1 (1985).
[100] 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. II 2008).
[101] *See* Jones v. United States, 529 U.S. 848, 858 (2000) ("We have cautioned … that 'unless Congress conveys its purpose clearly, it will not be deemed to have significantly changed the federal-state balance' in the prosecution of crimes." (quoting United States v. Bass, 404 U.S. 336, 349 (1971))).
[102] Economic Espionage Act of 1996, Pub. L. 104-294, Title I, § 101(a), 28 U.S.C. § 1367 (2006).
[103] *See* Theft of Trade Secrets, Crimes and Criminal Procedure, 18 U.S.C. § 1832 (2006).
[104] *See* Definitions, Crimes and Criminal Procedure, 18 U.S.C. § 1839(3)(A) &(B) (2006).

personal e-mail or surfing the web. Such activities are "the modern equivalent of getting up to stretch, or to talk briefly with a coworker. It is downtime, time spent recharging mental batteries."[105] However, an employee engaged in those activities would be accessing a protected computer without authorization[106] and would be obtaining information from the protected computer.[107] Similarly, an employee who uses a company cell phone to call his or her spouse might be subject to criminal liability.[108]

Although the government is unlikely to prosecute such minor violations, as the Court in *Nosal* stated, "we shouldn't have to live at the mercy of our local prosecutor."[109] Defining routine activities to be within the scope of the CFAA invites discriminatory and arbitrary enforcement.[110] It is also fathomable that the government will prosecute under the CFAA when it believes, but is unable to prove, that a defendant is guilty of a more serious crime. The threat of prosecution under the CFAA could be used to pressure a defendant to accept a plea even where the defendant was innocent of any other offense. Furthermore, the potentially broad coverage of the CFAA that results from the agency approach can enable employers to harass employees or competitors with civil suits.[111] In addition, "unauthorized" employees may be

---

[105] Kerr, *supra* note 7, at 1585.

[106] Doing personal business during business hours could be viewed as a breach of the employee's duty of loyalty.

[107] *See* 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. II 2008); *cf.* Clarity Servs., Inc. v. Barney, 698 F. Supp. 2d 1309, 1314 (M.D. Fla. 2010) (rejecting the agency approach, but suggesting that reading email would have been a violation of the Act under that approach).

[108] Cell phones are protected computers for purposes of the CFAA. *See* United States v. Kramer, 631 F.3d 900, 902-03 (8th Cir. 2011), United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005); Czech v. Wall St. on Demand, Inc., 674 F. Supp. 2d 1102, 1113 (D. Minn. 2009).

[109] United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.") (quoting United States v. Stevens, 130 S. Ct. 1577, 1591 (2010)).

[110] *Id.*

[111] *See Id.* at 860, n.6; P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 510 (3d Cir. 2005); Bashaw v. Johnson, No. 11-2693-JWL, 2012 WL 1623483 (D. Kan. May 9, 2012); Joseph Oat Holdings, Inc. v. RCM Digesters, Inc., 409 Fed. Appx. 498, 506 (3d Cir 2010). *See also* Nick Akerman, *CFAA Resembles RICO*, 27 NAT'L L.J. 13, 13 (Aug. 29, 2005) ("The Computer Fraud and Abuse Act … is fast becoming one of the most expansive and potent civil statutes in a civil litigator's arsenal….").

liable for civil damages for inadvertently causing damage or loss to their employers.[112] For example, if an employee accepts employment elsewhere or otherwise violates her duty of loyalty, she can be held responsible if she innocently causes the employer's system to crash even if the crash occurs while doing legitimate work for the employer.[113]

Finally, policy reasons do not support the agency approach. It is unnecessary to distort the statutory mandate of the CFAA to prevent theft of trade secrets. Traditional state actions for misappropriation, theft of trade secrets or breach of contract, are all available to deter improper conduct. Criminal prosecution is also available under state statutes[114] or the federal Economic Espionage Act.[115] These alternative means of combating the theft of trade secrets have the advantage of leaving federal courts unburdened by state claims, which are routinely attached to CFAA counts through supplemental jurisdiction.[116] Of course, the rule of lenity also counsels against adoption of the agency approach.[117]

B. Contract Approach

The contract approach is consistent with the statutory language of the CFAA. It is certainly possible to interpret "without authorization" or "exceeding authorized access" to encompass the violation of terms imposed as part of the authorization. However, the broad

[112] *See* 18 U.S.C. §§ 1030(a)(5)(C) & (g) (2006 & Supp. II 2008).
[113] *Id.; see also* 18 U.S.C. §§ 1030(e)(8) & (11) (2006 & Supp. II 2008).
[114] *See, e.g.*, ARK. CODE ANN, § 5-36 (West 2012); 18 PA. CONS. ANN. § 3930 (West 2012); TEX. PENAL CODE § 31.05 (West 2012).
[115] Economics Espionage, Crimes and Criminal Procedure, 18 U.S.C. §§ 1831-39 (2006).
[116] *See* Economic Espionage Act, 28 U.S.C. § 1367 (2006). There is no private right of action under the Economic Espionage Act, *see, e.g.*, Pisani v. Van Iderstine, No. CA 07-187S, 2007 WL 2319844, *3 (D. R.I. Aug. 9, 2007), so supplemental jurisdiction cannot be based upon that statute.
[117] *See supra* note 61.

contract approach,[118] much like the agency approach, appears inconsistent with Congressional intent and can lead to absurd, undesirable and possibly unconstitutional results.

As the contract approach is used to cover cases of employee theft of trade secrets,[119] it is susceptible to many of the same criticisms as the agency approach: (1) the definitions of damage and loss suggest that Congress did not intend the Act to cover misappropriation cases;[120] (2) the Act was designed to prohibit misconduct consummated on the computer, as opposed to prohibiting misconduct after information is obtained from a computer;[121] (3) application of the Act to trade secret cases would displace state common law absent any legislative intent to do so;[122] (4) enactment of the Federal Economic Espionage Act, which incorporates the traditional requirements of trade secret law and does not provide a private right of action, suggests that Congress affirmatively did not want the CFAA to displace state common law;[123] (5) minor employee transgressions could unknowingly lead to criminal prosecution;[124] (6) actions under state common law and the Economic Espionage Act are available to deter undesirable employee conduct without expanding the scope of the CFAA;[125] and (7) allowing trade secret cases to be brought under the CFAA will flood federal courts because they will be litigated as supplemental state claims.[126]

Application of the contract approach outside the employee context, such as in internet-related cases, presents a unique set of problems. Contract limitations to access can be used to

[118] I define "the broad contract approach" as finding access without authorization or in excess of authorization whenever *any* contract limitation is violated.
[119] *See, e.g.*, United States v. Nosal, 642 F.3d 781 (9th Cir. 2011), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).
[120] *See* 18 U.S.C. § 1030(e) (2006 & Supp. II 2008).
[121] *See* US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1189 (D. Kan. 2009).
[122] *See* Jones v. United States, 529 U.S. 848, 858 (2000).
[123] *See supra* notes 102-04 and accompanying text.
[124] Kerr, *supra* note 7, at 25.
[125] *See supra* notes 114-15 and accompanying text.
[126] *See supra* note 116 and accompanying text.

reduce marketplace competition.[127] A website's terms of use might prohibit access to the site by any competitor. An inability to quickly and cheaply obtain a competitor's pricing information could lead to marketplace inefficiencies and higher prices.

The contract approach also criminalizes trivial wrongs. Many dating websites prohibit posting inaccurate or misleading information.[128] Therefore, misstating one's age or weight or posting an outdated picture on such a site could be a violation of section (a)(4).[129] As stated earlier, until recently, Google forbade minors from using its service.[130] Minors who used Google to research a paper for school could have been prosecuted under section (a)(2)(C).[131] Employees using their work computers to shop online during lunch could be violating the Act if the company's policies contain the common prohibition against the use of company computers for non-business purposes.[132]

The rule of lenity, "which is rooted in considerations of notice,"[133] argues against adoption of the broad contract approach. "The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants."[134] Adopting the contract approach to interpret "without authorization" and "exceeding authorized access" definitely imposes such burdens. Few defendants read the terms

[127] *Cf.* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 578-79 (1st Cir. 2001) (plaintiff likely to succeed on merits where defendant used confidential information which permitted competitor to cheaply obtain pricing information on the plaintiff's website with a scraper program).
[128] *See* United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012).
[129] *See* 18 U.S.C. § 1030(a)(4) (2006 & Supp. II 2008). The requirement of fraudulent intent under that section does not require proof of common law fraud. Rather, it is enough to demonstrate the defendant's conduct was wrongful. *See* T-Mobile USA, Inc. v. Terry, No. 3:11-cv-5655-RBL, 2012 WL 1409287, at *6 n.1 (W.D. Wash. Apr. 23, 2012); *In re* Thundervision, LLC, No. 09-111 A, 2010 WL 2219352, at *12 (Bkrtcy. E.D. La. June 1, 2010); eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009).
[130] *See supra* note 75 and accompanying text.
[131] *See* 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. II 2008).
[132] *See* 18 U.S.C. §§ 1030(a)(2)(C) & (a)(4) (2006 & Supp. II 2008).
[133] LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2012) (quoting United States v. Romm, 455 F.3d 990, 1001 (9th Cir. 2006)).
[134] *Brekka*, 581 F.3d at 1134, *citing* United States v Santos, 553 U.S. 507, 514 (2008) (Scalia, J., plurality opinion).

of use of a website and those that do, often cannot understand them.[135] Worse still, many websites retain the right to change the terms of use at any time without providing notice of the change.[136]

This lack of notice may make section 1030(2)(a)(C) unconstitutionally void for vagueness under the contract approach .[137] "As generally stated, the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement...."[138] If "without authorization" and "in excess of authorization" are defined by private parties under terms of service, terms that are often unclear, unread, and subject to change without notice.,[139]"ordinary people" will not "understand what conduct is prohibited."[140] Additionally, under the contract approach, routine conduct becomes criminal. This impermissibly permits police officers and prosecutors to pursue their personal predilections concerning whom to arrest and prosecute.[141]

The contract approach raises troubling Constitutional questions beyond the void for vagueness doctrine. First Amendment issues could arise if the terms of use prohibit access for

[135] *See Nosal*, 676 F.3d at 862; Kerr, *supra* note 1, at 1659.
[136] *See Nosal*, 676 F.3d at 862.
[137] *See generally* United States v. Drew, 259 F.R.D. 449, 462-68 (C.D. Cal. 2009); Kerr, *supra* note 7, at 1573-78. In *Nosal*, the dissent, advocating the contract approach, acknowledged that approach might create vagueness problems under section 1030(a)(2)(C). *Nosal*, 676 F.3d at 866 (Silverman, J., dissenting). However, the dissent believed there was no vagueness issue under section 1030(a)(4), the section before the Court. *Id.* at 866-67. While the scienter requirement of section 1030(a)(4) alleviates vagueness concerns, a court's duty is to "construe statutes, not isolated provisions. Gonzales v. Carhart, 550 U.S. 124, 149 (2007); Gustafson v. Alloyd Co., Inc., 513 U.S. 561, 568 (1995). Given that "identical word and phrases within the same statute should normally be given the same meaning," Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007), and that a statute should be interpreted, where possible, to avoid constitutional infirmities, *See* Nat'l Fed. of Indep. Bus. v. Sebelius, 132 S. Ct. 2566, 2593 (2012); Harris v. United States, 536 U.S. 545, 555 (2002); INS v. St. Cyr., 533 U.S. 289, 299-300 (2001) (where the dissent wrongly ignored the possible vagueness problem under section 1030(a)(2)(C)).
[138] Kolender v. Lawson, 461 U.S. 352, 357 (1983).
[139] *See supra* notes 135-36 and accompanying text.
[140] *See Kolender*, 461 U.S. at 357.
[141] *See* Smith v. Goguen, 415 U.S. 566, 575 (1974).

the purpose of engaging in political speech or deny access to those with a particular viewpoint.[142] One commentator has also suggested that application of the contract approach in the internet setting may run afoul of the Intellectual Property Clause of the Constitution.[143] A basic tenet of statutory construction requires courts to avoid interpretations of statutes that raise Constitutional problems when alternative interpretations of the statute are fairly possible.[144] Constitutional problems aside, allowing private parties to limit access to public websites inhibits the free flow of information that the internet was designed to enhance.[145]

Finally, adoption of the contract approach is not necessary to hold computer users responsible for breaching a website's terms of use or company's employment policies. Traditional common law actions, such as breach of contract, misappropriation, or theft of trade secrets, can deter undesirable conduct. Again, without clear congressional intent, these common law actions should not be displaced..[146] Nor is it likely that Congress wished to flood federal courts with state actions that could be joined to a CFAA claim under supplemental jurisdiction.[147]

C. Plain Meaning Approach

The plain meaning approach is generally consistent with the statutory language. However, that approach assumes that language is unambiguous. More significantly, the language used to define "exceeding authorized access" in *WEC Carolina Energy Solutions LLC* [148] and some other "plain meaning" cases,[149] does not cover paradigm cases of computer fraud.

---

[142] *See* U.S. CONST. amend. I.
[143] *See* Galbraith, *supra* note 33, at 322, 324 n.35.
[144] *See Sebelius*, 132 S. Ct. at 2593; *Harris*, 536 U.S. at 555; *St. Cyr.*, 533 U.S. at 299-300.
[145] *See* Kerr, *supra* note 1, at 1650.
[146] *See supra* note 101.
[147] *See* 28 U.S.C. § 1367 (2006).
[148] 687 F.3d 199 (4th Cir. 2012).

As the *Brekka* court indicated,[150] the dictionary definition of authorization is permission. However, permission is not an unambiguous term. Permission can be limited or conditional. For example, assume a professor gives permission to a student to access his phone during class if he receives an emergency call from his pregnant wife. If the student accesses his phone to order a pizza, wouldn't access to the phone for that purpose be unauthorized? In short, the "plain meaning" approach cases generally do not explain why "authorization" should be interpreted to mean permission without considering limitations on that permission. [151]

Similarly, the "plain meaning" approach's definition of "exceeding authorized access" is not as "plain" as the approach suggests. For example, the Fourth Circuit and a number of courts adopting the "plain meaning" approach interpret the statutory definition of "exceeds authorized access" to apply to a person who is permitted to use the computer but who accesses information that he or she is not permitted to access.[152] "In other words, the term 'exceeds authorized access,' like the term 'access without authorization,' requires proof that the offender entered some forbidden virtual space…."[153] There are two problems with this definition. First, the definition does not indicate how one decides if the access extends beyond what is permitted: Is it determined by contract, by password or by some other way? Second, following the Fourth Circuit's interpretation, this would mean that a bank teller, who fraudulently alters an account that he or she is authorized to access and alter in other circumstances, would not be entering any

---

[149] *See* cases cited *infra* notes 152-53.
[150] LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, at 1133 (9th Cir. 2009).
[151] A few courts adopting the plain meaning approach have suggested that the plain meaning of the statute incorporates contract limitations, at least for the definition of "exceeds authorized access." *See* Farmers Bank & Trust, N.A. v. Witthuhn, No. 11-2011 –JAR, 2011 WL 4857926, at *5 (D. Kan. 2011); Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 385 (S.D.N.Y. 2010); *cf.* United States v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009) (adopting contract approach based on the statute's plain meaning).
[152] *See, e.g., WEC Carolina Energy Solutions*, 2012 WL 3039213, at *4; *Brekka*, 581 F.3d at 1133; Lewis-Burke, Assocs. v. Widder, 725 F. Supp. 2d 187, 195 (D.D.C. 2010); Orbit One Commc'ns v. Numerex Corp., 692 F. Supp. 2d 373, 385 n.67 (S.D.N.Y. 2010).
[153] *Univ. Sports Pub. Co.*, 725 F. Supp. 2d at 384.

forbidden virtual space and therefore, would not be violating section 1030(a)(4).[154] However, such conduct is precisely the type of computer fraud that should, and Congress undoubtedly intended to, be covered by the Act.

Criticizing existing approaches is easy. Developing a comprehensive alternative is more demanding. That is the challenge undertaken in the following section.

V. RECOMMENDED APPROACH TO DEFINING "WITHOUT AUTHORIZATION" AND "IN EXCESS OF AUTHORIZATION"

A. Defining "Without Authorization"

It is a "fundamental canon of statutory construction … that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning."[155] As the *Brekka* court found, the ordinary meaning of "without authorization" is "without permission."[156] The problem, as suggested above,[157] is that "permission" is an ambiguous term.

When faced with ambiguous statutory language, it is appropriate to look to the legislative intent.[158] There are several indications that Congress viewed unauthorized access as a trespass on another's computer.[159] After all, computer hacking "is akin to a trespass in cyberspace."[160] Thus, it is fitting to look at trespass law to define "without authorization."[161]

---

[154] *See* 18 U.S.C. § 1030(a)(4) (2006 & Supp. II 2008).
[155] Perrin v. United States, 444 U.S. 37, 42 (1979); Singh v. Attorney General of U.S., 677 F.3d 503, 510 (3d Cir. 2012).
[156] *See Brekka*, 581 F.3d at 1133.
[157] *See supra* notes 150-51 and accompanying text.
[158] *See* Blum v. Stenson, 465 U.S. 886, 896 (1984); Natural Res. Def. Council, Inc. v. FDA, No. 11 Civ. 3562 (THK), 2012 WL 983544, at *11 (2d Cir. Mar. 22, 2012).
[159] *See, e.g.,* S. REP. NO. 104-357, at 4, 11 (1996); S. REP. NO. 99-432, at 9 (1986).
[160] Kerr, *supra* note 1, at 1606.
[161] *Id.* at 1617-19.

The Model Trespass Statute states in part:

> A person commits an offense if, knowing that he is not licensed or privileged to do so, he enters or remains in any place as to which notice against trespass is given by:
> (a) actual communication to the actor; or
> (b) posting in a manner prescribed by law or reasonably likely to come to the attention of intruders; or
> (c) fencing or other enclosure manifestly designed to exclude intruders.[162]

Based partly on the language of the model trespass statute,[163] this article recommends that "accesses a protected computer without authorization" be defined as "to communicate with a protected computer without any permission, by circumventing code protection, e.g. password requirements, or after given specific notice that permission has been denied or revoked." The phrase, "without any permission," is designed to cover the computer hacker while excluding employees or persons accessing websites open to the public even if their access violates contractual limitations. Circumventing password or other code-based protection is the analogue to fencing, designed to exclude intruders. Specific notice corresponds with actual notice to the actor.

Despite the possible analogy to "posting in a manner prescribed by law or reasonably likely to come to the attention of intruders,"[164] the proposed definition of "without authorization" does not consider contract limitations to access. For the reasons provided in the discussion of the shortcomings of the "contract approach,"[165] broad contract limitations, such as restrictions on the use of information, cannot be allowed to define a person who accesses information "without authorization."

[162] MODEL PENAL CODE § 221.2(2) (2012).
[163] *See* MODEL PENAL CODE § 221.2 (2012).
[164] *Id*.
[165] *See supra* notes 118-47 and accompanying text.

A more difficult question is whether contractual limitations on access that are violated at the time of access should be considered to limit a person's authorization. For example, should access by a competitor or use of a robot be considered unauthorized when prohibited by a site's terms and conditions of use?

This article rejects consideration of even these more limited contract restrictions when determining if an access is "without authorization." As suggested earlier, terms of use are often unclear, seldom read and frequently subject to change without notice.[166] Accordingly, it is better to presume that notice "is not likely to come to the attention of intruders"[167] instead of incurring litigation costs to decide whether particular clickwrap or browserwrap agreements provide adequate notice.[168] The presumption that terms of use do not provide adequate notice is also justified by the rule of lenity:[169] a desire to keep the internet an open channel for information, and the ability of website owners to protect their interests by either individualized notice of lack of authorization or code protection.[170]

[166] *See Nosal*, 676 F.3d at 862; Kerr, *supra* note 1, at 1659.
[167] *See* MODEL PENAL CODE § 221.2(2)(b) (2012).
[168] Courts generally have held clickwrap agreements (where the user must manifest their consent) to be valid and browserwrap agreements (where terms are posted generally as a hyperlink) to be enforceable upon proof of actual or constructive notice, *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 20, 31 (2d Cir. 2002); Kwan v. Clearwire Corp., No. C09-1392JLR, 2012 WL 32380, at *7-8 (W.D. Wash. Jan. 3, 2012). However, these cases have arisen in the civil context. It is reasonable to demand a higher certainty that a party has received notice when faced with criminal prosecution. Although the CFAA also applies civilly, a statute which "has both criminal and noncriminal applications" should be construed consistently in the two contexts. Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004).
[169] *See supra* note 61. It is too easy to imagine a website's terms of use restricting access with vague language or for arbitrary reasons. *See* Kerr, *supra* note 1, at 1650 (hypothesizing a website that denies access to unfriendly or left-handed people).
[170] For example, if a site detects use of a robot, the source of the robot can be specifically notified that they are no longer permitted to access the site. Alternatively, the site can be coded to prevent access by robots. If the source of the robot circumvents that code, they would be guilty of unauthorized access. *Cf.* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (discussing trespass to chattels).

B. Defining "Exceeds Authorized Access"

The Act defines "exceeds authorized access" as "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."[171] Difficulty arises because the definition does not indicate when someone is entitled to alter or obtain information.

Under trespass law, consent is a defense precluding liability.[172] However, the defense is vitiated when the activity on the property is beyond the scope of the consent.[173] A party can exceed the scope of consent either by acting in a manner unnecessary to achieve the express or implied purpose of the consent or by violating explicit restrictions on the consent.[174]

By analogy to trespass law, this article recommends that the courts should interpret "exceeds authorized access" as referring to when a person obtains or alters information beyond what is necessary for the accomplishment of the general purpose for which access was initially authorized or in violation of prominent limitations on the type of information that can be obtained or altered. Once again, this article presumes that the notices in clickwrap and browserwrap agreements are not sufficiently prominent.[175] Violations of restrictions on the use of information, even if prominently displayed, would not "exceed authorized access" because the statutory definition focuses on obtaining or altering the information, acts that are consummated on the computer, not the information's subsequent use.

[171] 18 U.S.C. § 1030 (e)(6) (2006 & Supp. II 2008).
[172] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS §158, cmt. c (1985); RESTATEMENT (SECOND) OF TORTS § 892(a)(1) (1965); MODEL PENAL CODE § 221.2 (2012); Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505, 517 (4th Cir. 1999).
[173] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 892(a) (1965); *Food Lion, Inc.*, 194 F.3d at 517; Jacobini v. JP Morgan Chase, N.A., No. 611-cv-231-Orl-31GJK, 2012 WL 252437, at *3 (M.D. Fla. Jan. 26, 2012).
[174] *See* RESTATEMENT (SECOND) OF TORTS § 892A & cmt. g (2000).
[175] *See supra* note 168 and accompanying text.

This article rejects a strictly code-based interpretation of "exceeds authorized access"[176] because it conflicts with trespass law (where access beyond the scope of consent is improper even if the land improperly accessed is not fenced)[177] and is seriously under-inclusive. For example, if a person lends someone else their cell phone in an emergency, that should not permit the user to access naked pictures of the Good Samaritan's wife that have been saved on that phone. Similarly, a doctor that has access to patients' records at a hospital should not be allowed to review a patient's personal information who is not being treated by that doctor. Section 1030(a)(2) was designed to protect personal privacy,[178] and it is often impractical or inefficient to password-protect every individual piece of data on a computer. A code-based approach's under-inclusiveness is perhaps more troubling for actions brought under section 1030(a)(4). For example, a clerk who has access to account receivable files would not violate that section under a code-based approach even if she deleted customers' accounts (wiping out their debt) in return for kickbacks from the debtor. Surely Congress intended section 1030(a)(4) to cover such fundamental computer fraud.

C. Two Potential Problems with the Recommended Interpretation and the (Possibly Unnecessary) Legislative Remedy

The recommended interpretation has two potential shortcomings that result from the "plain meaning" of the statute. First, a literal reading of section (2)(a)(C)[179] would produce absurd results under the recommended interpretation. Second, the language of sections (a)(5)

[176] *See* Kerr, *supra* note 1, at 1663; *see also* Urban, *supra* note 53 at 1410 (recommending code-based approach with amendment to Section (a)(5)(A)); Field, *supra* note 53, 841-42 (2009) (recommending code-based approach as default option with possible modification by clear contract language).
[177] *See, e.g.,* RESTATEMENT (SECOND) OF TORTS §§ 158, cmt. c, 892A(1) cmt. g (2000).
[178] *See, e.g.,* S. REP. NO. 104-357, at 4 (1996); S. REP. NO. 99-432, at 6 (1986).
[179] *See* 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. II 2008).

and (e)(6)[180] seem to conflict with the recommendation of treating an employee who hacks into a code-protected part of the computer as unauthorized rather than as exceeding authorized access.[181] However, there are numerous reasons to reject such literal readings of the statute.

1. Limiting the Scope of Section 1030(2)(a)(C)

Section 1030(2)(a)(C) prohibits intentionally accessing a computer without authorization or in excess of authorization and by that means, obtaining information from any protected computer.[182] Under the recommended approach, an employee who uses a work computer for personal reasons has exceeded authorized access.[183] Such use is beyond that which is necessary to accomplish the purpose for which access was authorized. Therefore, an employee who surfs the web during lunch hour would be violating the literal reading of section 1030(a)(2)(C).[184] Such a result is untenable. However, the problem lies with the literal reading of that subsection, not with the recommended interpretation of the Act.

Section 1030(2)(a)(C) should be read to only prohibit obtaining private or confidential information without authorization or in excess of authorization. The legislative history contains multiple indications that section 1030(2)(a)(C) was designed to safeguard the protected computer owner's privacy, not public information.[185] Application of the Act without the suggested limiting interpretation would produce absurd results under any approach. For example, if a

[180] *See* 18 U.S.C. §§ 1030(a)(5) & (e)(6) (2006 & Supp. II 2008).
[181] *See supra* notes 163-68 and accompanying text.
[182] 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. II 2008).
[183] *See supra* notes 171-75 and accompanying text.
[184] *See* 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. II 2008). Courts have held that viewing material on the internet satisfies the "obtains information" requirement under section 1030(a)(2)(C). *See Drew*, 259 F.R.D. at 457; Healthcare Advocates, Inc. v. Harding, Early, Follmer & Frailey, 497 F. Supp. 2d 627, 648 (E.D. Pa. 2007); *see also* S. REP. NO. 99-432, at 6 (1986).
[185] *See, e.g.,* S. REP. NO. 104-357, at 7 (1996) ("The bill would amend section 1030(a)(2) to increase protection for the privacy and confidentiality of computer information."); S. REP. NO. 99-432, at 6 (1986) ("the premise of this subsection is privacy protection…").

patron goes behind the information desk at a bookstore to look up a title on the computer, she would be violating the law. A child who retrieves a text message from her parent's cell phone without permission would be a criminal.[186] Similarly, if a child, without asking, uses a friend's iPad to surf the web, she would be subject to prosecution. The Supreme Court has often emphasized that statutes should be interpreted to avoid such absurd results.[187]

Constitutional considerations also recommend the suggested limiting interpretation of section 1030(a)(2)(C). Criminalizing access to information raises First Amendment concerns. Although the right of access to information is not absolute, restrictions on access normally require a justification.[188] If the information is not private or confidential, it is difficult to justify section 1030(a)(2)(C)'s restraint, particularly given the punishment for unauthorized access in other sections of the Act.[189] The broad scope of section 1030(a)(2)(C) without the proposed limitation may also be unconstitutionally vague. Routine conduct can become criminal. This impermissibly allows police officers and prosecutors to pursue their personal predilections concerning whom to arrest and prosecute.[190] When possible, statutes should be interpreted to avoid such potential constitutional problems.[191]

This article advocates that the suggested limiting interpretation of section 1030(2)(a)(C) is appropriate. Congress did not intend that section to apply to non-private or publicly accessible information., Moreover, interpreting section 1030(2)(a)(C) to cover such information would

[186] Although such crimes are unlikely to come to the attention of prosecutors and be prosecuted, as the Court in *Nosal* stated, "we shouldn't have to live at the mercy of our local prosecutor." *See supra* notes 109-13 and accompanying text.
[187] *See, e.g.,* Corley v. United States, 556 U.S. 303, 317 (2009); Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 574-75 (1982); Perry v. Commerce Loan Co., 383 U.S. 392, 400 (1966).
[188] *See* ACLU of Mississippi, Inc. v. Mississippi, 911 F.2d 1066, 1072 (5th Cir. 1990) (citing Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978)); *In re* Application of Newsday, Inc., 895 F.2d 74 (2d Cir. 1990), *cert. denied*, 496 U.S. 931 (1990).
[189] *See, e.g.,* 18 U.S.C. §§ 1030(a)(4) & (a)(5) (2006 & Supp. II 2008).
[190] *See* Smith v. Goguen, 415 U.S. 566, 575 (1974).
[191] *See supra* note 137.

produce absurd, and possibly unconstitutional, results under any approach . Nonetheless, to ensure the proper interpretation of that section, it is recommended that Congress amend section 1030(a)(2) by inserting the words "private or confidential" before "information" in subsection (C).

2. Treating Employees as Unauthorized Rather than Exceeding Authorized Access When They Hack Into a Code-protected Part of a Protected Computer

The definition of "exceeds authorized access" appears to cover employees who hack into code-protected parts of their work computer. [192] An employee is authorized to access his work computer but by hacking into a code-protected part of the computer, she obtains information in the computer that she is not entitled to obtain. Despite the language of section 1030(e)(6), there are several reasons to treat such an employee as unauthorized rather than exceeding authorized access.

The only practical consequence under the Act that results from the classification of exceeding authorized access, as opposed to unauthorized access, is avoidance of liability for unintentional damage or loss under sections 1030(a)(5)(b) & (c).[193] Yet, the risk of loss or damage should be on an employee who hacks into a code-protected part of the computer. The employer's adoption of code protection for internal parts of the computer suggests that the risk of loss or damage from access is real. At a minimum, it indicates that the employer has taken reasonable steps to notify employees that access to the code-protected parts of the computer are unauthorized. An employee who knowingly and intentionally goes where she does not belong,

[192] *See* 18 U.S.C. §§ 1030(e)(6) (2006 & Supp. II 2008).
[193] *See* 18 U.S.C. §§ 1030(a)(5)(B) & (C) (2006 & Supp. II 2008).

as opposed to violating a non-explicit understanding of authorized access, should be responsible for the loss or damage she creates.

Treating the employee hacker as unauthorized is also consistent with trespass law. As suggested earlier, password or other code protection is the equivalent of fencing under the Model Trespass Statute.[194] It provides notice that the employee is not entitled to enter the code-protected realm and that doing so without consent constitutes a trespass. The Restatement (Second) of Torts also suggests that improper access to a code-protected part of the computer should be treated as a trespass. Section 158, comment c states, in part, "If the possessor of land gives a consent to the actor's presence upon only a particular part of his land, the actor's intentional entry upon any other part of the land is an intrusion, and, if unprivileged, is a trespass."[195] The legislative history suggests that Congress intended section 1030(a)(5) to "criminalize[] *all* computer trespasses."[196]

Finally, literally interpreting the language of section 1030(e)(6) would produce undesirable results that could not have been intended in the Internet context. A person is always permitted to access a site's public homepage. If the site requires a password to go further, a person who hacks into the site should be responsible for any damage or loss she creates. On the other hand, with the literal application, a hacker would only be liable under section 1030(a)(5) for intentional damage because she would merely be exceeding authorized access since she was initially authorized to access the protected computer through the home page.

Although this article argues that an employee-hacker can be reasonably treated as unauthorized, as opposed to merely exceeding authorization, the language of the Act suggests

[194] *See supra* notes 161-64 and accompanying text.
[195] RESTATEMENT (SECOND) OF TORTS § 158, cmt. c (1965).
[196] S. REP. NO., 104-357, at 11 (1996) (emphasis added).

otherwise. Thus, legislative amendment would be desirable to remove any doubt. It is recommended that the Act be amended to include the following definition:

The term "accesses a computer without authorization" means to use or communicate with a protected computer either

a) without any permission,
b) by circumventing password or other code protection, or
c) after individual notice that permission has been denied or revoked.

D. Advantages of the Suggested Approach

The recommended interpretation of the CFAA is consistent with the language of the statute and most closely coincides with Congressional intent to limit coverage of the Act to crimes consummated on the computer.[197] The suggested approach covers core computer crimes – theft of private information, fraudulent alteration of data, and intentional or unauthorized damage to computer systems or data – but neither co-opts state common law claims nor clogs federal courts with supplemental state claims. The approach does not impose liability without clear knowledge of culpability, but provides mechanisms (password protection or individualized denial or revocation of access) to computer owners to protect their interests. It best balances the individual's right to privacy and the public's interest in free and open access to information. Unlike existing law in many circuits, this article's interpretation of the Act does not raise Constitutional problems or violate the rule of lenity. Finally, the recommended approach is relatively easy to apply because unlike some other approaches, it does not consider subjective intent.

[197] *See supra* note 95.

E. Illustrations of Application of the Suggested Approach

1. An associate at a law firm uses her work computer to check the weather for the weekend – the employee has exceeded authorized access (because the access was not necessary for work), but there would be no violation because the information obtained would not be private or confidential. Without the suggested limiting interpretation to section 1030(a)(2)(C), there would arguably be a violation under every approach.

2. A secretary surfing the web during the work day downloads a file which contains a worm that causes the company computer a loss of more than $5,000 – the employee has exceeded authorized access but is not responsible for the damage because the damage was unintentional. Under the agency approach, and possibly the contract approach,[198] the access is unauthorized and the employee would be liable for the loss as well as subject to criminal prosecution.

3. A salesperson accepts employment with her employer's competitor and e-mails confidential customer lists to the competitor – the salesperson is authorized to access the customer lists for her job, so the access is neither unauthorized nor exceeding authorized access. Therefore, the salesperson would not have violated the CFAA. The salesperson could be liable under common law theories, such as breach of contract or theft of trade secrets. Under the agency and contract approaches, the salesperson would likely be criminally liable under the CFAA. This would be true even if the employer did not take reasonable steps to maintain the information's confidentiality.

4. The salesperson in the prior example deletes all of their files before leaving for the new job – the salesperson is authorized to access the computer; whether she has exceeded

[198] Whether there is a violation under a contract approach depends on the terms of the contract. This will be true for most of the examples analyzed in this part.

authorization depends upon whether the salesperson is authorized to delete files as part of her job. However, whether the salesperson is unauthorized or exceeding authorization should not be significant. The salesperson should be liable under section 1030(a)(5) for intentional damage to the computer and would not have violated sections 1030(a)(2) & (a)(4), even if unauthorized.

5. A system's administrator at a University, who is also taking classes at the school, accesses a professor's computer and reads a copy of the final exam – access to the professor's computer is authorized by the system's administrator, but reading the exam is not necessary for the job and therefore, it exceeds authorized access. There would be a violation of the Act as the information obtained is private or confidential. This would not be a violation under either Professor Kerr's strictly code-based approach (because no code was violated)[199] or the Fourth Circuit's plain meaning approach (because access to the information was authorized).

6. A company uses a robot to obtain pricing information from its competitor's public website – without more, the company is authorized to use the site and has not exceeded authorized access. It could still be liable for intentional damage to the competitor's computer if knowledge could be imputed to the company that the competitor's system would be damaged by the use of the robot.[200] The company's access would be unauthorized if: either the company circumvented code protection against use of a robot or, the competitor, after detecting the use of the robot, notified the company that it was no longer authorized to use the site. If unauthorized, there would still be no violation of section 1030(a)(2) because the information is not private or

[199] *See* Kerr, *supra* note 1 (a strictly code-based approach requires an authorized user to improperly access code-protected information to exceed authorized access).

[200] Intention might be imputed to the company if it understood the likely effects of its actions – that making an extremely large number of search requests would slow down the competitors operations. *Cf.* Pulte Homes, Inc. v. Laborers' Int'l. Union, 648 F.3d 295, 303 (6th Cir. 2011) (finding intentional conduct where the defendant sent e-mails at such a volume that it should have understood the likely effects of its conduct was to slow the plaintiff's computer system, although the court also found that such likely effect was probably one of the defendant's objectives). However, this would be a difficult standard to meet given evidence that most uses of robots do not interfere with a system's operations. *See* Galbraith, *supra* note 33, at 333.

confidential. However, there would be liability under section 1030(a)(5) for any damage or loss, even if unintentional.

7. A single woman intentionally misstates her age and weight on a computer-dating site, which she accesses with a valid password.– The woman is authorized to use the site and has not exceeded authorized access. However, if the misstatements are reported to the dating site, they could ban the woman from further access to the site, making such later access unauthorized. Based on the terms of most dating sites, the initial access is unauthorized or in excess of authorization under a contract approach. Arguably, if the access is unauthorized or exceeding authorized access, there would be a violation of sections 1030(2)(a)(C) and (a)(4).[201]

VI. CONCLUSION

Although few attorneys and even fewer laypeople are familiar with the CFAA, litigation under the Act has dramatically increased.[202] Despite the large number of cases that have been decided, the Courts have not agreed upon a proper interpretation of the Act. A majority of the Circuit Courts of Appeals that have interpreted the Act have read it broadly, apparently wishing to ensure that disloyal employees are punished under the Act. Such interpretations are not dictated by the language of the statute and are inconsistent with the legislative history of the Act. Broad interpretation of the Act raises Constitutional problems, violates the rule of lenity, can inhibit competition, displaces state law without any clear Congressional intent to do so, increases the number of supplemental state claims brought to federal court, and threatens to result in liability for common and accepted conduct. Reliance on prosecutorial discretion to choose which

[201] The unauthorized access could provide private information about another site user. It also might be considered fraud under section (a)(4) that resulted in obtaining something of value – a date, possibly with expenses paid. 18 U.S.C. § 1030 (2006 & Supp. II 2008).

[202] A Westlaw search of cases containing "CFAA" during the decade of the 1990's returned just four cited case. By contrast, in just the first two years of the current decade, the same search revealed 189 cited cases.

cases to bring is not an acceptable solution, particularly when civil litigators have also begun to abuse the Act.[203]

Given the availability of common law actions to punish the disloyal employee, there is no reason to suffer the consequences of some Circuit Courts' broad reading of the statute. Instead, this article has recommended a narrow interpretation of the CFAA which builds upon the "plain meaning" approach, that has been adopted by the Fourth and Ninth Circuits, and derives, in part, from analogy to trespass law. Persons "without authorization" would include outsiders (those without any permission), those who have circumvented password or other code protection, and anyone who has been individually notified that their access has been denied or revoked. A person would "exceed authorized access" when she obtains or alters information either beyond that necessary to accomplish the general purpose for which access was granted or in violation of prominent limitations on the type of information that can be obtained or altered. In addition, the proposed interpretation of the Act would limit section 1030(a)(2)(c) to unauthorized access or access in excess of authorization of private or confidential information. This article's recommendations avoid the pitfalls of the existing approaches to the Act, prohibit the core computer crimes that Congress intended to be covered under the Act,[204], and optimally balances an individuals' interest in privacy with the public's interest in free and open communications on the Internet. Although this article argues that the proposed approach to the Act is a valid interpretation of the existing law, minor legislative amendments are recommended to maximize the likelihood that all courts concur.

[203] *See supra* note 111.
[204] *See supra* note 159. See also A.V. *ex. rel* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2008) (the CFAA is "a statute generally intended to deter computer hackers").