Exceeding authorized access in the workplace: Prosecuting disloyal conduct under the Computer Fraud and Abuse Act

Authors: Stephanie M. Greene, Christine Neylon O'Brien

Persistent link: http://hdl.handle.net/2345/bc-ir:103632

This work is posted on eScholarship@BC, Boston College University Libraries.


These materials are made available for use in research, teaching and private study, pursuant to U.S. Copyright Law. The user must assume full responsibility for any use of the materials, including but not limited to, infringement of copyright and publication rights of reproduced materials. Any materials used for academic research or otherwise should be fully credited with the source. The publisher or original authors may retain copyright to the materials.
If you spend time at work checking Facebook or shopping online you might be violating your employer’s computer policy. But you might also be committing a federal crime. For the past decade or so, courts have disagreed over the scope of the Computer Fraud and Abuse Act. Computers provide new opportunities for distraction at work; they also provide opportunities for dishonest behavior. While some behavior is clearly criminal, it is not always clear what type of behavior should be criminal under the Act, particularly as social norms about workplace habits and computer use are constantly evolving. Some courts have found that an employee who violates a workplace policy, breaches a contract, or breaches a duty of loyalty to his employer may be both civilly and criminally liable under this Act if such misconduct involves a computer.

This article focuses on how courts have construed the Computer Fraud and Abuse Act which criminalizes some types of access to computers, detailing how courts continue to struggle with an accepted interpretation of what is, and what is not, criminal. A recent highly anticipated case, the Ninth Circuit’s en banc United States v. Nosal decision, reflects this discord. In a 9-2 decision, the court held that the ambiguous criminal statute should be given limited applicability because its general purpose is to punish hacking rather than conduct such as misappropriation of confidential information. The decision expresses concern that a broad interpretation of the statute would criminalize a range of acts we all engage in on employer networks. The Ninth Circuit’s interpretation creates a notable split of opinion with the First, Fifth, Seventh and Eleventh circuit courts of appeal. In a case involving civil charges under the CFAA, the Court of Appeals for the Fourth Circuit agreed with the Ninth Circuit’s narrow interpretation of the Act.

I. INTRODUCTION

Computers have introduced new distractions and new temptations into the workplace. Employees may use work time to shop, socialize or gamble on employers’ computers even though such behavior is prohibited by the employer computer use policies or by employment agreements. As computer use has grown and employees work from home or remote locations, the line between what is appropriate computer use and what is a
violation of an employer’s computer use policies has blurred.¹ What repercussions should employees suffer if they violate employer computer use policies? Some violations may be de minimis whereas others might pose substantial threats to employers – such as harm to reputation or exposure of confidential information. In the most extreme cases, employees may use employer computers to commit crimes. Thus, misuse of employers’ computers encompasses a broad spectrum of behavior from lazy employees who squander time at the computer, to scheming criminals.

The sections of the Computer Fraud and Abuse Act (CFAA) at issue prohibit accessing computers “without authorization” or “exceeding authorized access.”² While this language was largely intended to prohibit both external and internal hacking,³ both employers and prosecutors have argued, and some courts have agreed, that this language also prohibits conduct such as violating a computer use policy or other employment agreement. Some may argue that employers and prosecutors are unlikely to pursue minor violations of computer use policies, but courts are mindful that a broad interpretation of the CFAA could support cases that involve conduct that Congress did not intend to criminalize.⁴

¹ See Ed Frauenheim, Stop reading this headline and get back to work, July 11, 2005, CNET/NEWS, http://news.cnet.com/Stop-reading-this-headline-and-get-back-to-work/2100-1022_3-5783552.html (last visited May 19, 2012) (discussing web survey of 10,000 employees conducted by salary.com and web portal America Online that showed surfing the web was the largest time waster at work; that most employees spend more than two of their eight work hours on personal, non-work matters); see also Andrew T. Hernack, War, Terror, and the Federal Courts, Ten Years After 9/11: 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, 1544-48 (2012)(noting widespread use of cellphones, smartphones, and mobile devices with mobile applications and arguing that broad interpretation of unauthorized access under CFAA violates the vagueness doctrine and due process).


³ See discussion infra at Part VI.A. See also LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009); Int’l Assoc. of Machinists and Aerospace Workers v. Werner-Matsuda, 290 F. Supp. 2d 479, 495-96 (D. Md. 2005). Hacking is used to describe a variety of compromises to networked computers, ranging from innocuous customizations (“modding”), to circumventing security protocols, and further, criminal acts done to systems that perpetrate even more harm. See Fernando M. Pinguelo & Bradford Muller, Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals, 16 VA. J. L. TECH. 116, 131-32 (2011); Daniel Lippman & Julian Barnes, Malware Threat to Internet Corralled, WALL ST. J., July 9, 2012, available at http://online.wsj.com/article/SB10001424052702303292204577515262710139518.html.

⁴ See Part II A & B discussing a broad interpretation of the Computer Fraud and Abuse Act. While the cases courts have considered to date have involved serious transgressions, Part IV of this article discusses the en banc decision of the Court of Appeals for the Ninth Circuit in United States v. Nosal, where the majority noted that the less serious transgressions would be subject to the same analysis and consequences as more serious infractions. 676 F.3d 854, 862 (9th Cir. 2012). See also WEC Carolina Energy Solutions,
This article refers to disloyal employees to describe those whom employers or the government have targeted as violating the CFAA because they have misappropriated confidential information, violated a computer use policy, or breached an employment contract. Such acts of employee disloyalty have traditionally been the province of contract and tort law, with employers suing disloyal employees for misappropriation of trade secrets, conversion, unfair competition, and tortious interference with a business expectancy.

Trade secret law frequently provides a remedy to employers when employees steal confidential information. Primarily a creature of state law, trade secret statutes protect all manner of business methods, devices, techniques, customer lists, costs, prices, margins, and strategic plans that businesses keep secret in order to maintain a competitive advantage.

5 See Greg Pollaro, Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope, 2010 DUKE L. & TECH REV. 12, at ¶3 (2010) (concluding “CFAA was not designed to apply to employer/employee claims that are traditionally handled under state tort and contract law”). It should be noted that egregious disloyalty may be proffered as a defense by employers who have disciplined or discharged employees for engaging in concerted activities that are protected by section 7 of the National Labor Relations Act. See Christine Neylon O’Brien, The First Facebook Firing Case Under Section 7 of the National Labor Relations Act: Exploring the Limits of Labor Law Protection for Concerted Communication on Social Media, 45 SUFFOLK UNIV. L. REV. 29, 49-58 (2011) (discussing the Supreme Court’s ruling in NLRB v. Local Union No. 1229 (Jefferson Standard), 346 U.S. 464, 476-77 (1953) that an employer need not retain an employee when conduct is so disloyal to employer that it provides a separate cause for discharge); cf. Matthew W. Finkin, Disloyalty! Does Jefferson Standard Stalk Still?, 28 BERKELEY J. EMP. & LAB. L. 541, 551-57 (2007) (questioning value of disloyalty as a standard and noting it chills speech of social value).

The concept of disloyalty is based upon the agency concept that an employee owes a duty of loyalty to his or her employer. See Charles A. Sullivan, Mastering the Faithless Servant?: Reconciling Employment Law, Contract Law, and Fiduciary Duty, 2011 WIS. L.REV. 777, 777-78, 806 (noting that the most recent Restatement of Agency (Third) (2006) views employees as a species of agent). An employee violates the duty of loyalty owed to the employer when the employee does not act solely for the benefit of the employer in matters connected to the agency/employment and, in such cases, the employer may recover secret profits as well as wages paid during the period of disloyalty. See Marisa Warren & Arnie Pedowitz, Practitioner’s Note: Social Media, Trade Secrets, Duties of Loyalty, Restrictive Covenants and Yes, The Sky is Falling, 29 HOFTSR LA. & EMP. L.J. 99, 105 (2011) (discussing cases relying upon the Restatement (Second) of Agency). Numerous statutory employment protections are limited by the concept that even if an employee has engaged in protected activity, he or she may nonetheless be subjected to discipline and/or discharge for separate unprotected activities that provide an independent cause for discipline. Thus, engaging in protected activities, or being a member of a protected class, does not provide carte blanche for employee misbehavior, including that which is disloyal to the employer. In the context of CFAA cases, the agency-based interpretation of authorization is perhaps best illustrated in the Seventh Circuit’s decision in International Airport Centers v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006), discussed infra Part III. See Matthew Kapitanyan, Beyond WarGames: How the Computer Fraud and Abuse Act Should be Interpreted in the Employment Context, 7 I/S J. L. & POL. 405, 423 (2012) (discussing Citrin as “marquee case for agency-based interpretation of authorization”).

competitive advantage. The Economic Espionage Act (EEA) of 1996 criminalizes theft or misappropriation of trade secrets related to a product in foreign or interstate commerce. The EEA however, contains no private right of action.

The CFAA does provide a private right of action and therefore it has increasingly been used to sue employees whose misconduct or disloyalty has some relationship with a computer. Thus, numerous cases involving misappropriation of confidential information have been brought under the CFAA. In such cases, employers typically allege that an employee has acted “without authorization” or has “exceeded authorized access” by breaching an employment policy, or a contract that includes a confidentiality or noncompete agreement. Increasingly, the Department of Justice has also sought to use the CFAA to prosecute crimes involving employees who violate employment policies or agreements. The CFAA not only has the advantage of federal jurisdiction, but the statute’s minimal requirements may make it easier for an employer or the government to make its case. As the number of such cases has grown, the courts have struggled to determine the extent to which the CFAA is an appropriate vehicle for holding disloyal employees accountable in both civil and criminal contexts.

In 2012, the Court of Appeals for the Ninth Circuit issued an en banc decision emphasizing that the CFAA is “an anti-hacking statute” and not “an expansive

---

10 See Thomas E. Booms, Note, Hacking into Federal Court: Employee “Authorization” Under the Computer Fraud and Abuse Act, 13 VAND. J. ENT. & TECH. L. 543, 544-46 (2011) (noting increasing workplace computer use and employers looking to CFAA to prevent insiders from misappropriating confidential information and seeking monetary relief from disloyal employee misappropriation).
11 See id. at 557-58 (discussing courts that have adopted broad view that employee misuse vitiates authorization).
14 See Brenton, supra note 9, at 430-31 (noting CFAA does not contain the same proof requirements as trade secret law and disrupts delicate equilibrium between employer and employees); see also R. Mark Halligan, Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996, 7 J. MARSHALL REV. OF INTELL. PROP. L. 656, 673-75 (2008) (discussing use of CFAA in the trade secret context and need for private right of action under EEA).
misappropriation statute.”\textsuperscript{15} In \textit{United States v. Nosal}, the Ninth Circuit held that an employee who misappropriates an employer’s confidential information does not “exceed authorized access” within the meaning of the CFAA.\textsuperscript{16} The Ninth Circuit was the first of the circuit courts of appeal to interpret the CFAA so narrowly.\textsuperscript{17} The Court of Appeals for the Fourth Circuit has since agreed with the Ninth Circuit’s “narrow and literal” interpretation of the Act.\textsuperscript{18} Other circuit courts of appeal have read the statute more broadly, finding employees guilty or liable under the CFAA for either breach of a confidentiality agreement, an employment policy, or a duty of loyalty, reasoning that such transgressions satisfy the requirement of acting “without authorization” or “exceeding authorized access.”\textsuperscript{19}

For several years, the broad interpretation of the CFAA seemed to predominate, as decisions in the First, Fifth, Seventh, and Eleventh Circuits found employees could be accountable under the CFAA for a variety of computer-related misconduct.\textsuperscript{20} Chief Judge Kozinski’s savvy opinion in \textit{United States v. Nosal} however, marshals the arguments that several district courts and scholars have made against broad use of the CFAA.\textsuperscript{21} The Ninth Circuit appears to be at the forefront of a new trend that recognizes dangers in the CFAA as a catch-all statute to pursue or prosecute employees for fraudulent or disloyal use of workplace computers.

This article considers whether the CFAA should be used by employers or prosecutors to pursue employees who violate an employment policy, contract, or duty of loyalty. Part I explores the rise of the use of the CFAA to sue or prosecute employees who misappropriate confidential information. Part II summarizes the debate over the broad and narrow interpretations that have been ongoing in the federal courts over the past twelve years. Part III focuses on the development of the \textit{Nosal} case in the Ninth Circuit to

\textsuperscript{15} \textit{United States v. Nosal}, 676 F.3d 854, 857 (9th Cir. 2012) [hereinafter \textit{Nosal IV}]. \textit{See supra} note 3 and accompanying text discussing hacking.

\textsuperscript{16} \textit{Nosal IV}, 676 F.3d at 857.

\textsuperscript{17} \textit{Id.} at 863 (“respectfully declin[ing] to follow our sister circuits….”).

\textsuperscript{18} \textit{WEC Carolina Energy Solutions v. Miller}, 687 F.3d 199, 203 (4th Cir. 2012).

\textsuperscript{19} \textit{See United States v. Rodriguez}, 628 F. 3d 1258, 1263-64 (11th Cir. 2010), \textit{cert. denied}, 131 S. Ct. 2166 (2011) (CFAA violated due to employer policy breach); \textit{United States v. John}, 597 F.3d 263, 270-73 (5th Cir. 2010) (CFAA violated for breach of the duty of loyalty based on unlawful use of material lawfully accessed); \textit{Int’l Airport Ctrs., LLC v. Citrin}, 440 F.3d 418, 420-21 (7th Cir. 2006) (CFAA violated for unlawful access when agency relationship terminated due to breach of employment contract and breach of duty of loyalty); \textit{EF Cultural Travel BV v. Explorica, Inc.}, 274 F.3d 577 581-82 (1st Cir. 2001) (CFAA violated based on terms of broad confidentiality agreement prohibiting access to employer information). The Second Circuit’s stance on CFAA cases is possibly in flux at this time. \textit{Compare United States v. Morris}, 928 F.2d 504 (2d Cir. 1991) (finding CFAA violation for unauthorized access) \textit{with United States v. Aleynikov}, 676 F.3d 71 (2d Cir. 2012) (noting that district court dismissed CFAA charge on grounds that “authorized use of a computer in a manner that misappropriates information is not an offense under the Computer Fraud and Abuse Act”). \textit{See infra} Part IV.

\textsuperscript{20} \textit{See United States v. Rodriguez}, 628 F.3d 1258, 1263-64 (11th Cir. 2010), \textit{cert. denied}, 131 S. Ct. 2166 (2011) (CFAA violated when employee viewed information for a nonbusiness purpose); \textit{United States v. John}, 597 F.3d 263, 271 (5th Cir. 2010) (CFAA violated when employee used information with purpose of committing fraud); \textit{Int’l Airport Ctrs., LLC v. Citrin}, 440 F.3d 418, 420-21 (7th Cir. 2006) (CFAA violated when employee exceeded authorized access by breaching duty of loyalty to employer); \textit{EF Cultural Travel BV v. Explorica, Inc.}, 274 F.3d 577, 581-82 (1st Cir. 2001) (CFAA violated based on breach of broad confidentiality agreement).

\textsuperscript{21} \textit{Nosal IV}, 676 F.3d at 860-63.
expose how both the narrow and broad interpretations of “without authorization” and “exceeds authorized access” are applied to the same set of facts. Part IV identifies the notable circuit split that the Ninth and Fourth Circuits’ interpretations create with the First, Fifth, Seventh and Eleventh circuit courts of appeal. Part V defends the Ninth Circuit’s reasoning. Part VI suggests that the trend to follow the narrow view will continue and that employers should, therefore, consider more traditional tort and contract methods of pursuing disloyal employees. Part VI also considers changes that Congress might consider in revising relevant portions of the CFAA. We conclude that all circuits should follow the narrow interpretation of the authorization terms of the statute or that Congress should amend the CFAA to clarify the scope of prosecution authorized under the Act.

II. THE CFAA HAS GROWN FROM AN ANTI-HACKING STATUTE TO A STATUTE ENCOMPASSING EMPLOYEE COMPUTER MISUSE

The Computer Fraud and Abuse Act, 18 U.S.C. §1030 (2012), 22 protects computers in which there is any federal interest and specifically outlaws conduct that victimizes computer systems. 23 The initial iteration of the law as enacted in 1984, addressed a smaller subset of acts, most particularly hacking into computers. 24 Congress continually amended and expanded the CFAA both in its reach and mandate. 25 The CFAA now protects computer systems from trespassing, threats, damage, espionage, or even being used as instruments of fraud and identity theft. 26 Beyond the government’s right to file suit for damage, civil claims were added in a 1994 amendment providing for private rights of action. 27 The CFAA provides remedies for a wide range of acts against computers, and overlaps with portions of the Economic Espionage Act as well as state laws. 28

The CFAA prohibits:

1. computer trespassing (hacking) in a government computer, 18 U.S.C. §1030(a)(3);

---

25 Andreano, supra note 24, at 85-87.
28 See Brenton, supra note 9 (discussing the statutes’ redundancies with state laws).
2. computer trespassing resulting in exposure to governmental, credit or computer-housed information, 18 U.S.C. § 1030(a)(2);
3. damaging a bank or government computer, or those used in interstate commerce, 18 U.S.C. § 1030(a)(5);
4. committing fraud, an integral part of which involves unauthorized access to such computers, 18 U.S.C. § 1030(a)(4);
5. threatening to damage such computers, 18 U.S.C. § 1030(a)(7);
6. trafficking in passwords for such computers, 18 U.S.C. § 1030(a)(6);
7. accessing a computer to commit espionage, 18 U.S.C. § 1030(a)(1)
(Assertion and conspiracy to commit these crimes are prohibited by 18 U.S.C. §1030(b)).

Congress developed a two-tier approach for sentencing penalties under the CFAA. First offenses are set at one level, and are enhanced for subsequent violations. Punishments for violating the CFAA range from fines to imprisonment for up to twenty years, or both.

Those provisions usually invoked in cases involving an employee’s misappropriation of confidential information are sections 1030(a)(2)(C), 1030(a)(4) and 1030(a)(5)(C). Section 1030(a)(2)(C) is violated when an individual “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” Section 1030(a)(4) prohibits accessing a protected computer without authorization or exceeding authorized access knowingly and with intent to defraud to obtain something of sufficient value. Section 1030(a)(5)(C) punishes one who “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.”

While it is clear that the CFAA is primarily a criminal statute, the 1994 amendment allows a private party to bring a civil suit “to obtain compensatory damages and injunctive relief or other equitable relief” if he “suffers damage or loss by reason of a violation” of the Act. Thus, violation of any of the CFAA’s provisions, as outlined above, may expose an individual to both civil and criminal liability. Compensatory and equitable relief is available in a civil action, provided a violation causes any one of the following five classes of loss or damage:

---

32 See generally Obie Okuh, Comment, When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access, 21 ALB. L.J. SCI. & TECH. 637, 650 & n.59 (2011)
35 The 1994 amendments were part of an omnibus crime bill. See Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001(b), 108 Stat. 1796, 2097-98 (1994). Section 1030(g) provides in relevant part: “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.” See Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 MINN. L. REV. 1561, 1563-71 (2010) (detailing the expansion of the CFAA) [hereinafter Vagueness Challenges].
(I) losses exceeding $5,000;
(II) impairment to medical records;
(III) physical injuries;
(IV) threats to public health or safety;
(V) damage to government interest computer systems.  

Later amendments in 1996 and 2008 further broadened the definition of “protected computers,” increasing the range and number of computers covered by the CFAA to include any computer connected to the Internet. Most crucially, these amendments allow suits by private employers against employees who misuse workplace computers.

In both civil and criminal cases, a determination of liability or guilt hinges largely on whether an individual has accessed a computer “without authorization” or has “exceeded authorized access.” Violations of the CFAA use either one or both terms. “Without authorization” is not defined by the statute. “Exceeds authorized access” is defined as “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.” Courts have strained to develop a coherent approach to the statute that gives meaning to both phrases – “without authorization” and “exceeds authorized access.”

Courts that interpret this language to apply primarily to hackers construe the term “without authority” as applying to outsiders who hack into computer systems, with no authority whatsoever to access the computer or computer system; and the term “exceeding authorized access” as applying to insiders who have access but exceed permitted limits. It is clear that employees who exceed limits based on a breach of code-based security have exceeded authorized access.

---

37 See 18 U.S.C. §1030(e)(2) (2012). The definition was amended to include computers “used in interstate commerce or communication.” Id. A further amendment changed the definition to include computers “used in or affecting interstate or foreign commerce or communication,” signaling Congress’s intent that it be able to regulate to the full extent of its Commerce Clause power. See Kerr, Vagueness Challenges, supra note 35, at 1570.
38 See cases cited supra at note 19.
42 See, e.g., WEC Carolina Energy Solutions v. Miller, 687 F.3d 199, 204 (4th Cir. 2012)(“[r]ecognizing that the distinction between these terms is arguably minute”).
43 For a discussion of hackers and insiders who exceed authorized access, see Part VI infra.
44 See Kerr, Cybercrime’s Scope, supra note 4, at 1643 (recommending use of breach of code-based access as trigger for “exceeding authorized access”). Such transgressions may also be identity theft. See Office of Legal Educ., Exec. Office for U.S. Attys, Dep’t of Justice, Computer Crime and Intell. Prop. Section, Criminal Div., Prosecuting Computer Crimes 22 (2007) available at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf. [hereinafter DOJ Prosecution Manual] (discussing identity theft). Other crimes that damage computers or computer systems are also prohibited by the CFAA such as inserting worms and distributing denial-of-service attacks. See Kerr, Cybercrime’s Scope, supra note 4, at 1603-04 (discussing these damaging acts); see also DOJ Prosecution Manual, supra note 44 (noting virus or worm can use up all available bandwidth on employer’s computer network thus denying employees access and delete files, crash computer, install malicious software, and in general do
Because the language of the CFAA is so broad, it is susceptible to interpretations encompassing other types of computer misuse beyond hacking. Some courts have held that employees who breach confidentiality agreements or commit acts adverse to their employers’ interests have acted “without authorization” or have “exceeded authorized access” within the meaning of the statute. 45 A variety of theories have justified such interpretations. For example, some courts have used an agency theory, reasoning that employees have authorized access based solely on their status as agents of their employers. 46 Under this theory, employees lose their status as agents, and are “without authorization” when their interests diverge from those of their employer. 47

Whether the statute is read narrowly to focus on acts such as hacking, or more broadly to encompass employee misappropriation of confidential information, depends entirely on the interpretation of the phrases “without authorization” and “exceeds authorized access.” Professor Orin Kerr, an authority on the CFAA, expressed concern that expansive interpretations of the critical terms “without authorization” and “exceeds authorized access” in civil cases would be applied in criminal cases. 48 Kerr opines that such broad interpretations ultimately give prosecutors too much discretion in determining when employees may be charged under the CFAA. 49

The circuit court split over interpretations of the CFAA language is rooted in different views of the Act’s purpose. Courts urging adoption of a narrow view of the Act emphasize that its primary purpose is to punish hacking. 50 Courts taking a broader view emphasize that the statute has been amended and expanded to broaden its mandate, and thereby focuses on punishing an increasing variety of acts related to computer misuse. 51 The following section traces the development of the broad reading of the terms “without authorization” and “exceeds authorized access” through leading cases. The section then illustrates how the theories developed in civil cases were adopted for use in criminal cases.

45See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 581-82 (1st Cir. 2001) (CFAA violated based on terms of broad confidentiality agreement prohibiting such access to employer information).

46See Int’l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (CFAA violated for unlawful access when agency relationship terminated because employee breached duty of loyalty by destroying files that were employer property).

47Id. at 421 (referring to Restatement (Second) of Agency §§112, 387 (1958), and Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124 & n.3 (W.D. Wash. 2000)).

48See Kerr, Cybercrime’s Scope, supra note 4, at 1641.

49See Kerr, Vagueness Challenges, supra note 35, at 1576-77 (characterizing CFAA as “breathtakingly broad” and arguing that courts must adopt a meaning of unauthorized access that limits “discretion of law enforcement authorities to bring charges at whim” and “does not let police arrest whomever they like . . . any typical computer user”).

50See LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009); Int’l Assoc. of Machinists and Aerospace Workers v. Werner-Matsuda, 390 F. Supp. 2d 479, 495-96 (D. Md. 2005).

51See cases collected supra at note 19 and accompanying text; see also NCMIC Finance Corp. v. Artino, 638 F. Supp. 2d 1042, 1058-59 (S.D. Iowa 2009) (arguing that legislative history supports liability for misappropriation of confidential information); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127-29 (same).
III. DEVELOPMENT OF THE BROAD AND NARROW INTERPRETATIONS

A. Civil Cases using the Broad Interpretation

The availability of civil remedies changed the CFAA landscape considerably. By 2000, courts had recognized that Congress’s 1994 amendment to the CFAA added a private cause of action under section 1030(g). By 2003, the United States Court of Appeals for the Third Circuit observed that although most CFAA cases still involved “classic hacking activities,” the reach of the statute had expanded. The court noted that employers “are increasingly taking advantage of the CFAA’s civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer’s computer system.”

One of the first cases to address the broadened scope of the CFAA in the civil context was heard by the Court of Appeals for the First Circuit in 2001. Like most civil cases under the CFAA, the case involved disloyal employees who sought to enrich themselves by supplying information from a former employer to a competitor. The case involved a dispute between EF Cultural Tours, which specialized in world tours for high school students, and a newcomer to the field, Explorica. Several EF employees left the company to work for Explorica. An EF employee, using his knowledge of the company’s website, directed an Explorica employee to design a robot-like computer program called a scraper to gather pricing information from EF’s website. Using this process, Explorica was able to obtain extensive information about EF’s pricing to undercut those prices and thereby gain an unfair competitive advantage. Explorica and former employees of EF were charged with violating section 1030(a)(4) which prohibits obtaining anything of value by accessing a protected computer without authorization or exceeding authorized access knowingly and with intent to defraud. Although the court recognized that Explorica could have gathered the various codes manually through repeated searching, it was convinced that the employee had exceeded authorized access because the scheme “reek[ed] of use –and, indeed, abuse – of proprietary information . . . .”

The court focused on the confidentiality agreement that EF employees voluntarily entered into, an agreement that clearly prohibited sharing the company’s proprietary information. The court skirted the issue of whether the employees were “without authorization,” emphasizing instead that they had exceeded authorized access. The court concluded that an employee exceeds authorized access when he breaches a broad confidentiality agreement.

---

52 Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124 & n.3 (W.D. Wash. 2000). In 2003, the Court of Appeals for the Ninth Circuit recognized that the CFAA could provide a civil remedy to a third party whose computer was accessed without authorization, because the statute states that “any person who suffers damage or loss” may recover. Theofel v. Farey-Jones, 341 F.3d 978, 986 (9th Cir. 2003).


54 See id.

55 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).


57 EF Cultural Travel, 274 F.3d at 583.
agreement.\textsuperscript{58} According to the court, Explorica may have had some authorization “to navigate around EF’s website (even in a competitive vein)” but “it exceeded that authorization by providing proprietary information . . . to create the scraper.”\textsuperscript{59}

The Court of Appeals for the Seventh Circuit used the law of agency to interpret the extent of an employee’s authorization. In \textit{International Airport Centers v. Citrin}, the court found that an employee is “without authorization” once he violates a duty of loyalty to his employer.\textsuperscript{60} The employee was entrusted with a company laptop to identify potential real estate acquisitions. After accumulating the data, the employee left his employer to start his own business.\textsuperscript{61} He deleted the files from the laptop before returning it to his former employer and loaded a secure erasure program that prevented the recovery of the deleted files.\textsuperscript{62} The employee allegedly violated section 1030 (a)(5)(A)(1) which prohibits transmitting a program that “intentionally causes damage \textit{without authorization} to a computer.”\textsuperscript{63} Thus, the Seventh Circuit had to confront the term “without authorization” directly, as exceeding authorized access is not mentioned in this section of the CFAA. The court found that the employee was authorized to use the laptop, but that his authorization ended once he decided to leave the company and to destroy files.\textsuperscript{64}

In attempting to construe the phrase “without authorization,” the Seventh Circuit raised the issue of differentiating between the terms “without authorization” and “exceeds authorized access.” The court characterized the difference as “paper thin . . . but not quite invisible.”\textsuperscript{65} Nevertheless, the court made little attempt to confront the implications of the two distinct terms. The court stated that “exceeding authorized access” seemed a better description of what the employee in \textit{Citrin} did but moved on to conclude that the employee was “without authorization” because all authorization ended once he violated his duty of loyalty to his employer.\textsuperscript{66} According to the court, the only basis for authority to access the employer’s computer was the agency relationship which terminated when the employee violated a duty of loyalty by failing to disclose his adverse interests.\textsuperscript{67} It is unclear from the court’s analysis how the agency relationship and breach of a duty of loyalty impacts an employee who exceeds authorized access.

The agency theory adopted in \textit{Citrin} was more precisely articulated in 2000 in \textit{Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.}\textsuperscript{68} In \textit{Shurgard}, the district court cited the Restatement (Second) of Agency in interpreting the meaning of “authorization.”\textsuperscript{69} Restatement section 112 provides: “Unless otherwise agreed, the

\textsuperscript{58} \textit{Id.} at 581.
\textsuperscript{59} \textit{Id.} at 583.
\textsuperscript{60} \textit{Int’l Airport Ctrs., LLC v. Citrin}, 440 F.3d 418, 419 (7th Cir. 2006).
\textsuperscript{61} \textit{Id.}
\textsuperscript{62} \textit{Id.}
\textsuperscript{63} \textit{Id.} (citing 18 U.S.C. §1030(a)(5)(A)(1) (2012) (emphasis added)).
\textsuperscript{64} \textit{Citrin}, 440 F.3d at 420.
\textsuperscript{65} \textit{Id.} (citations omitted).
\textsuperscript{66} \textit{Id.} at 419.
\textsuperscript{67} \textit{Id.} at 420-21.
\textsuperscript{68} 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).
\textsuperscript{69} \textit{Id.}
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.”

Many federal district courts have followed the agency approach adopted in Shurgard and Citrin, emphasizing that authorization arises only from the contractual or agency relationship.

B. Criminal Cases using the Broad Interpretation

Writing in 2003, Professor Orin Kerr was disturbed by decisions that found employees had acted without authorization or had exceeded authorized access under the CFAA because they had breached either an implied or an explicit contract. Kerr worried that such broad interpretations of the terms “without authorization” and “exceeds authorized access” would be applied to criminal cases, thereby “threaten[ing] a dramatic and potentially unconstitutional expansion of criminal liability in cyberspace.” At that time, the First Circuit had held that an employee exceeds authorized access by breaching an employment agreement and the Shurgard decision had engendered a host of decisions favoring a broad reading based on the agency theory that an employee loses authorization once he acts contrary to the interests of his employer. When the Seventh Circuit decided Citrin in 2006, holding that an employee’s authorization terminates when he breaches a duty of loyalty, the broad reading appeared to be gaining momentum. Professor Kerr’s concerns proved prescient. In 2010, both the Fifth and Eleventh Circuit Courts of Appeal interpreted the CFAA broadly in criminal cases that sought to punish employees who knowingly violated contractual terms or employment policies.

The Court of Appeals for the Fifth Circuit concluded that an employee who is authorized to access information exceeds that authorization if her intent was to use the information to perpetrate a crime. In United States v. John, an employee of Citigroup accessed

---

70 Restatement (Second) of Agency § 112 (1958).
72 Kerr, Cybercrime’s Scope, supra note 4, at 1599, 1637-39. Professor Kerr also noted some of the analytical problems presented in the earliest case decided under the CFAA, that of United States v. Morris, 928 F. 2d 504 (2nd Cir. 1991). Id. This was a criminal case involving not a disloyal employee, but an outside hacker. Morris unleashed a worm on a computer that he was authorized to use but his intent to access computers that he was not authorized to access was implied because he knew that the worm would invade computers that he was not authorized to access. Id. He used weaknesses in programs to obtain access in unintended ways. Id. at 1632. Thus Morris’ use of the computer that he was authorized to use was an unintended, as opposed to an intended use, and was “without authorization.” Id. The intended function test used by the Second Circuit to indict Morris was not adopted by other courts. Id. at 1630-32. See also discussion of U.S. v. Morris infra at text accompanying notes 207-11.
73 See Kerr, Cybercrime’s Scope, supra note 4, at 1599.
74 See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001); Field, supra note 71 , at 820.
76 United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).
confidential customer information and used that information to commit fraud. She was charged with violating section 1030(a)(2). John contended that the statute prohibits using authorized access to obtain or alter information that she is not entitled to alter, but that it does not prohibit unlawful use of material that was gained through authorized access. Rejecting this argument, the court reasoned that the employee had access to certain information for limited purposes and that she exceeded authorized access when she intended to use the information for other purposes. The court focused not only on the employee’s criminal intent and purpose but also on the fact that she was aware of company policies and knowingly violated those policies.

The Court of Appeals for the Eleventh Circuit held that an employee exceeds authorized access if he accesses information for a nonbusiness reason, in violation of the employer’s computer use policy. Rodriguez was charged with violating section 1030 (a)(2)(B), which prohibits accessing information “from any department or agency of the United States” without authorization or in excess of authorized access. As part of his job as a TeleService representative with the Social Security Administration, Rodriguez had access to Administration databases that contained sensitive personal information including social security numbers, addresses, dates of birth, and annual income. He accessed information about seventeen individuals who were acquaintances or relatives. Unlike the defendant in John, Rodriguez did not use this information for criminal purposes. Instead, he used the information to send letters, birthday cards, or flowers to female acquaintances. The Administration had clearly communicated its policy prohibiting an employee from obtaining information from its databases without a business reason. Employees were informed about this policy through mandatory training sessions; notices were posted in the office; and a banner appeared on every computer screen daily. The Administration warned employees that they faced criminal penalties if they violated policies on unauthorized use of databases.

In finding that Rodriguez had exceeded his authority under the CFAA, the Eleventh Circuit emphasized that Rodriguez had violated the employer’s policy. The Court was not persuaded by Rodriguez’s argument that he did not use the information for a criminal purpose and that he did not defraud anyone or seek any financial gain in exceeding his authorized access. The Court concluded that the statute is clear that merely accessing the information by exceeding authorized access is criminal. The Eleventh Circuit also rejected the defendant’s argument that the Fifth Circuit’s decision in John required some intent to use the information in furtherance of a crime. According to the court, “his use

77 Id.
78 Id.
79 Id. at 272.
80 Id. at 273.
81 United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).
82 Id. at 1260. Rodriguez appears to have accessed the information to satisfy his curiosity about relatives. He also used the information to send flowers or letters to women he was interested in pursuing. Id. at 1261-62.
83 Id. at 1260.
84 Id. at 1263.
85 Id.
86 Id.
of the information is irrelevant if he obtained [it] without authorization or as a result of exceeding authorized access.\textsuperscript{87}

The decisions by the Fifth and Eleventh Circuits indicate the breadth that the CFAA may have in the criminal context. Like courts that read the CFAA broadly in the civil context, the courts found that employees may be prosecuted for exceeding authorized access when they knowingly violate an employer’s policy or when they have the intent to misuse the information. The next section traces the development of a more narrow interpretation of the terms “without authorization” and “exceeds authorized access.” This narrow interpretation focuses on whether or not employees had permission to access information, rather than on their intent or subsequent use of the information.

C. Narrow Interpretations in Civil Cases: LVRC Holdings v. Brekka

As cases seeking to hold disloyal employees accountable under the CFAA grew in number, some federal district courts resisted the broad interpretation of “without authorization” and “exceeds authorized access,” that developed in the First, Fifth, Seventh, and Eleventh Circuits.\textsuperscript{88} Courts favoring a narrow view emphasized the plain meaning of the statute, the legislative history that emphasizes the anti-hacking focus of the Act, and the need to observe the principles of the rule of lenity.\textsuperscript{89}

The Ninth Circuit was the first circuit court of appeals to adopt a narrow view of authorization under the CFAA. In 2009, the Ninth Circuit decided \textit{LVRC Holdings v. Brekka},\textsuperscript{90} a decision which set forth the reasoning the court ultimately employed in its en banc decision in \textit{United States v. Nosal}, with both the plain language approach and the rule of lenity figuring prominently in the court’s reasoning. In \textit{Brekka}, the court emphasized that it is the employer’s actions rather than the employee’s state of mind that determines whether the employee had authorized access to the computer.\textsuperscript{91}

Brekka, an employee at an addiction treatment center, was negotiating for an ownership interest in the business. When negotiations broke down, Brekka left to start a competing business. Before leaving, he emailed several documents to his personal email accounts.\textsuperscript{92} LVRC alleged that Brekka violated sections 1030(a)(2) and (4) of the CFAA. The court

\textsuperscript{87} \textit{Id.} at 1263. In \textit{United States v. Teague}, the Court of Appeals for the Eighth Circuit upheld the conviction of a woman who allegedly used her privileged access to the National Student Loan Data System to access President Obama’s student loan records. 646 F.3d 1119 (8th Cir. 2011). Teague was convicted under sections 1030(a)(2)(B) and (c)(2)(A) of the CFAA and sentenced to two years probation. \textit{Id.} at 1120. The appeal did not address whether she had “exceeded authorized access” but rather whether she had the right to a computer expert to review certain discovery documents. The court found that Teague did not demonstrate that the expert was necessary to her defense. \textit{Id.} at 1123-24.


\textsuperscript{89} See \textit{id.}

\textsuperscript{90} 581 F.3d 1127 (9th Cir. 2009).

\textsuperscript{91} \textit{Id.} at 1135.

\textsuperscript{92} \textit{Id.} at 1129-30.
considered whether Brekka had acted “without authorization” or “exceeded authorized access” under the CFAA in emailing the documents to his personal computer. The court found that an employee does not act “without authorization” or “exceed authorized access” when he transfers an employer’s confidential information to his own personal computer to further his own personal interests. In interpreting these terms, the court sought a “sensible interpretation” that gave meaningful effect to both terms. Because the statute does not define “without authorization,” the court looked to its plain meaning, finding that “authorization” turns on whether an employer has granted the employee permission to use the company’s computer. Thus, the court found that “without authorization” means that an individual had “no rights, limited or otherwise, to access the computer in question.” The court cited hackers and employees whose access has been rescinded or terminated as those “without authorization.”

Recognizing that “exceeds authorized access” must have a meaning distinct from “without authorization” and relying on the statutory definition, the court concluded that a person “exceeds authorized access” if he is authorized to use a computer for certain purposes but goes beyond limitations imposed by the employer. The court found that there was no evidence that Brekka acted “without authorization” or “exceeded authorized access” when he emailed the documents to his personal computer because he had his employer’s permission to use the computer, as well as permission to access and obtain the information in question.

The court noted that its interpretation of terms in the CFAA had to be consistent in both civil and criminal cases. The rule of lenity which advises against interpreting “criminal statutes in surprising and novel ways that impose unexpected burdens on defendants,” gave further support to a narrow interpretation of the terms “without authorization” and “exceeds authorized access.” The court found that a broad interpretation of these

---

93 The employer alleged that the employee had violated sections 1030(a)(2) and (4). Id. at 1131. Section 1030(a)(2)(C) provides for criminal penalties against a person who: “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication . . . .” 18 U.S.C. §1030(a)(2)(C) (2012). Section 1030(1)(4) provides for criminal penalties against a 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 . . . .” 18 U.S.C. § 1030(a)(4) (2012).
94 581 F.3d at 1136-37. The case also considered whether Brekka was “without authorization” in accessing the company’s website after he left the employer. The court stated that if he had done so he would have acted “without authorization” but there was insufficient evidence to determine that Brekka had accessed the website after he left the employer.
95 Id. at 1133.
96 Id.
97 Id.
98 Id. at 1135.
99 Id.
100 Id. at 1128.
101 Id. at 1134.
102 Id.
phrases would not adequately notify employees about the range of acts considered criminal.\textsuperscript{103}

Although the Ninth Circuit’s decision in \textit{Brekka} marked a distinct difference in the approach the circuits were taking to interpreting the CFAA, the cases at the court of appeals level were different enough to allow some room for distinction. Thus in \textit{United States v. John}, the Court of Appeals for the Fifth Circuit recognized “that the Ninth Circuit may have a different view of how ‘exceeds authorized access’ should be construed,”\textsuperscript{104} but suggested nonetheless that its decision could be read consistently with the Ninth Circuit’s decision in \textit{Brekka}.\textsuperscript{105} The Fifth Circuit’s decision noted that in \textit{Brekka}, the court was concerned that an employee might be unaware that his authorization had terminated and it would, therefore, be unfair to subject him to criminal penalties for personal use of an employer’s computer.\textsuperscript{106} In \textit{John}, however, there was no such unfairness or uncertainty the court reasoned, because an employee who is using information for criminal or fraudulent purposes is well aware that she is exceeding authorized access.\textsuperscript{107} The Fifth Circuit suggested that \textit{Brekka} can be read to imply that “when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer’s policies and is part of an illegal scheme, it would be ‘proper’ to conclude that such conduct ‘exceeds authorized access’ within the meaning of the CFAA.”\textsuperscript{108}

The Eleventh Circuit also sought to distinguish its decision in \textit{Rodriguez} from \textit{Brekka}. Like the Fifth Circuit, the Eleventh Circuit noted that an employee’s knowledge about his violation of a policy or agreement makes a critical difference. Thus, because Brekka was not bound by any employment agreement that prohibited employees from emailing company documents to personal email accounts,\textsuperscript{109} he was in a different position than Rodriguez who knew he was not authorized to obtain personal information for nonbusiness reasons.\textsuperscript{110}

The Court of Appeals for the Sixth Circuit, however, gave some weight to the narrow view articulated in \textit{Brekka}. In \textit{Pulte Homes v. Laborers’ International Union},\textsuperscript{111} the court interpreted the term “without authorization” narrowly. After an employee was fired from Pulte Homes, the labor union initiated a phone and email blitz that disrupted Pulte’s

\begin{footnotes}
\item[103] Id. at 1135.
\item[104] 597 F.3d at 272.
\item[105] Id. at 273.
\item[106] Id.
\item[107] Id.
\item[108] Id.
\item[109] Rodriguez, 628 F.3d at 1263 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009)).
\item[110] See id.
\end{footnotes}
system. Pulte alleged that the union violated section 1030(a)(5)(B) of the CFAA which prohibits intentionally accessing a computer without authorization. The court found that the blitz was not “without authorization” under the CFAA because these systems were “open to the public” and thus access was not “unauthorized.” The court cited *Brekka* for giving a plain language meaning to the term “without authorization” and also for the importance of recognizing that “without authorization” and “exceeds authorized access” must have different meanings. The court concluded that “without authorization” means “no permission to access whatsoever.”

Before the Ninth Circuit Court of Appeals decided *United States v. Nosal*, two schools of thought had developed on how to interpret the terms “without authorization” and “exceeds authorized access.” The first read the statute broadly in both civil and criminal cases, finding that employees were without authorization or exceeded authorized access if they violated employment agreements, confidentially agreements, or computer use agreements. This view emphasized that employees who had acted contrary to the interests of their employer lost any authority they might have had. Courts adopting this broad reading of the statute made little attempt to distinguish between the terms “without authorization” and “exceeds authorized access.” The second school of thought found that the statute should be read literally and narrowly, especially as the statute applies both civilly and criminally. Under the narrow view, courts emphasized that the appropriate inquiry is whether or not the individual had permission to access the material in question, not whether he had the intent to subsequently misuse the material. Courts adopting the narrow view stressed that the terms “without authorization” and “exceeds authorized access” must have distinct meanings, a fact which further supported a more literal interpretation. Before *Nosal*, the narrow view had been applied only in civil cases. Thus, *Nosal* provided an opportunity for the Ninth Circuit to confront the scope of the CFAA in cases involving criminal prosecution for disloyal behavior using a computer.

**IV. THE NOSAL DECISION**

In *United States v. Nosal*, the Court of Appeals for the Ninth Circuit had an ideal opportunity to address the questions that were surfacing between the circuits. The facts in *Nosal* were similar to those in *Brekka*, *EF Cultural*, and *Citrin*, involving an employee who stole a former employer’s information. But the case was raised in the criminal context. Would the court find that an employee who breached employment contracts or a duty of loyalty to his employer could be prosecuted under the CFAA? Following on the heels of *Brekka*, the *Nosal* case gave the Ninth Circuit the opportunity to consider the interpretation of “without authorization” and “exceeds authorized access” more closely than any other circuit. While the reasoning in *Brekka* eventually carried the day, the following sections show the great vacillation in the Ninth Circuit’s challenge to

---

112 Pulte, 648 F.3d at 299.
113 Id. at 304.
114 Id. at 303-04.
115 Id. (citing Lockheed Martin Corp. v. Speed, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. Aug. 1, 2006)).
116 Nosal IV, 676 F.3d 854 (9th Cir. 2012). See supra note 19 and accompanying text.
117 Nosal IV, 676 F.3d at 856.
118 Id.
adopt the broad or narrow view.\footnote{Id. at 859-61.} The summary of the Ninth Circuit’s en banc decision reveals that the court answered any lingering questions about the reach of the \textit{Brekka} decision and clearly defined the parameters of the terms “without authorization” and “exceeds authorized access.”\footnote{Id. at 855-61.}

\subsection*{A. United States v. Nosal – The District Court and Ninth Circuit Decisions – Interpretations Both Broad and Narrow}

The \textit{Nosal} case, like \textit{Brekka}, involved employees who stole confidential information from an employer to set up a competing business. \textit{Nosal}, however, was a criminal case. The facts of the case date back to 2004 and 2005. David Nosal worked for Korn/Ferry, an executive search firm. His employment with the firm ended in 2004 but he signed an agreement to work as an independent contractor for Korn/Ferry for several months as well as a noncompete agreement.\footnote{United States v. Nosal, No. C 08-0237 MHP, 2010 U.S. Dist. LEXIS 24359, at *3 (N.D. Cal. Jan. 6, 2010) [hereinafter \textit{Nosal II}].} In violation of these agreements, Nosal conspired with several Korn/Ferry employees to gain access to confidential information that he used to set up his competing executive search firm. Nosal was indicted for trade secret theft, mail fraud, and violations of the CFAA.\footnote{United States v. Nosal, No. CR 08-00237 MHP, 2009 U.S. Dist. LEXIS 31423 (N.D. Cal. Apr. 13, 2009) [hereinafter \textit{Nosal I}].} The CFAA count was based on section 1030(a)(4) which punishes one who “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access . . . .”\footnote{18 U.S.C. § 1030(a)(4) (2012).} The government maintained that Nosal violated this section by aiding and abetting the Korn/Ferry employees in exceeding their authorized access with intent to defraud.\footnote{\textit{Nosal II}, 2010 U.S. Dist. LEXIS 24359, at *3.} Although the employees had unrestricted access to the computers in question, the government argued that access was limited to legitimate use of the information accessed.\footnote{\textit{Id.} at **18-20.} The United States District Court for the Northern District of California originally adopted the broad interpretation of “without authorization” and “exceeds authorized access,” finding that Nosal violated the CFAA.\footnote{\textit{Id.} at *18-20.} The court found that Nosal exceeded authorized access because he accessed his employer’s computer and confidential information with “nefarious intent,” meaning interests contrary to those of his employer or in violation of his employment agreement.\footnote{\textit{Id.} at *10 (citing \textit{Nosal I}, 2009 U.S. Dist. LEXIS 31423, at **6-7).}

After the Court of Appeals for the Ninth Circuit decided \textit{Brekka}, the district court reconsidered its decision in \textit{Nosal}.\footnote{\textit{Nosal II}, 2010 U.S. Dist. LEXIS 24359, at *2.} Building on the distinction the court made in \textit{Brekka} between the terms, “without authorization” and “exceeds authorized access,” it found that the statutory definition of “exceeds authorized access” means that it must consider “intent” and “authorization” as “separate elements of the CFAA.”\footnote{\textit{Id.} at *16.} Looking at the
statutory definition of “exceeds authorized access,” the court stated that “a person only ‘exceeds authorized access’ if he has permission to access a portion of the computer system but uses that access to ‘obtain or alter information in the computer that [he or she] is not entitled so to obtain or alter.’”\textsuperscript{130} The court concluded that the statute cannot reasonably be read to allow “alter” to mean “misappropriate.”\textsuperscript{131} Thus, the court applied the reasoning in \textit{Brekka} to find that Nosal’s co-conspirators did not exceed authorized access even though they violated their employer’s confidentiality and terms of use agreements.\textsuperscript{132}

In 2011, a three-judge panel of the United States Court of Appeals for the Ninth Circuit reversed the district court’s decision.\textsuperscript{133} The court held 2-1, that “an employee exceeds authorized access when he or she obtains information from the computer and uses it for a purpose that violates the employer’s restrictions on the use of the information.”\textsuperscript{134} In construing the definition of “exceeds authorized access,” the court focused its attention on the pivotal word “so.” The definition provides that an employee exceeds authorized access when he uses authorized access “to obtain or alter information in the computer that the accesser is not entitled \textit{so} to obtain or alter.”\textsuperscript{135} The court used a dictionary definition of “so” to mean “in a manner or way that is indicated or suggested.”\textsuperscript{136} Thus, the court concluded that an employee who accesses information in a manner to which he is not entitled, has exceeded authorized access.\textsuperscript{137}

The court distinguished the situation in \textit{Nosal} from \textit{Brekka}, reasoning that Brekka did not act without authorization and did not violate any access restrictions because there was no written employment agreement or guidelines prohibiting emailing business documents to a personal computer.\textsuperscript{138} By contrast, Nosal and the Korn/Ferry employees were subject to a clear and conspicuous computer policy with specific restrictions.\textsuperscript{139}

Furthermore, the three-judge panel found that the rule of lenity which supported its narrow interpretation of terms in \textit{Brekka} did not apply to \textit{Nosal}.\textsuperscript{140} The Korn/Ferry employees had knowledge of the employer’s limitations, the court stated, and “certainly had fair warning that they were subjecting themselves to criminal liability.”\textsuperscript{141} The situation in \textit{Brekka} was different according to the court, because there was no policy or employer action that gave the employee adequate notice that authorization was limited or revoked.\textsuperscript{142}

\begin{footnotes}
\footnotenum{130} Id. at *20 (citing 18 U.S.C. §130(e)(6) (2012)).
\footnotenum{132} Id. at *22.
\footnotenum{133} United States v. Nosal, 642 F.3d 781 (9th Cir. 2011) [hereinafter \textit{Nosal III}].
\footnotenum{134} Id. at 782.
\footnotenum{136} \textit{Nosal III}, 642 F.3d at 785.
\footnotenum{137} Id. at 785-86.
\footnotenum{138} Id. at 787.
\footnotenum{139} Id.
\footnotenum{140} Id. at 786-87.
\footnotenum{141} Id. at 787-88.
\footnotenum{142} Id. at 786.
\end{footnotes}
B. The Ninth Circuit’s En Banc Decision – The Narrow Interpretation Prevails

In 2012, the Court of Appeals for the Ninth Circuit reconvened for an en banc hearing in *Nosal* and reversed the panel’s decision. The court held 9-2 that the CFAA does not extend to violations of an employer’s use restrictions, reasoning that Congress must legislate more clearly if it wants to incorporate misappropriation liability into the CFAA. 143 Rejecting the uncomfortable distinction its former decision had attempted to make between *Brekka* and *Nosal*, the court stated that the CFAA was intended to cover only unauthorized access to computers, such as “hacking,” not unauthorized use of information. 144 Impermissible access, the court reasoned, must be determined by considering whether an employee has “circumvent[ed] technological barriers.” 145

In reaching this conclusion, the court paid close attention to principles of statutory construction, but its overriding concern was the potential for haphazard or overbroad application of the statute in criminalizing a wide variety of daily computer use. The Ninth Circuit’s decision is peppered with examples of how employees use workplace computers for personal reasons in violation of an employer’s computer use policy - such as sending personal emails, checking sports scores, or playing Sudoku. 146 The court noted that employees are seldom disciplined for violating computer use policies, and therefore cautioned that a broad interpretation of the CFAA would create precedent for employers to threaten to report minor violations by “troublesome employees” to the FBI. 147 The court stated that “[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.” 148

The court cited several problems associated with interpreting the CFAA including violations of employers’ computer use policies or websites’ terms of service. First, the court noted that the CFAA should not be used to criminalize behavior and relationships that have traditionally been regulated by tort and contract law. 149 Second, the court characterized computer use policies and terms of service as broad, vague, opaque, subject to change, and frequently unknown. 150 Such characteristics, the court noted, raise serious questions regarding adequate notice to employees about what constitutes criminal behavior. 151 For example, the court asked, what does “nonbusiness” use mean? 152 Finally, the court stated that the breadth and vagueness of use policies and terms of service leave too much discretion to prosecutors and juries, potentially leading to arbitrary enforcement of the statute. 153 These problems, inherent in a broad interpretation

---

143 *Nosal IV*, 676 F.3d at 862-64.
144 *Id.* at 859, 863.
145 *Id.* at 863-64.
146 *Id.* at 860-61.
147 *Id.* at 859-60.
148 *Id.* at 861.
149 *Id.* at 860.
150 *Id.* at 860-61.
151 *Id.* at 862.
152 *Id.* at 860-61.
153 *Id.* at 862.
of the CFAA, are magnified, according to the court, because other devices used in daily life such as smart phones, iPads and Kindles, involve “access to remote computers . . . governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands.”

The court cited a few examples of the far-reaching effects a broad reading of the CFAA could have. In United States v. Drew, the defendant was prosecuted under the CFAA for creating a false profile on MySpace.com.\(^{155}\) In lying about the information in the profile, the defendant violated MySpace’s terms of service, thereby subjecting her to a claim that she exceeded authorized access under the CFAA.\(^{156}\) In a civil case, an employer counterclaimed in a wrongful termination suit, alleging that the employee had violated the CFAA by checking Facebook and sending personal email in violation of company policy.\(^{157}\) Although the CFAA claims were dismissed in both of these suits, the Ninth Circuit cited these examples to illustrate the potential for misuse or abuse of the statute. Despite the unlikelihood that the government would pursue minor violations, the court stated, “we shouldn’t have to live at the mercy of our local prosecutor.”\(^{158}\)

While the focus of the Ninth Circuit’s decision is that a broad reading of the CFAA could turn “minor dalliances” into “federal crimes,”\(^{159}\) the decision includes careful analysis of the statutory language and legislative history. The court rejected the government’s attempt to read the definition of “exceeds authorized access” to include use restrictions.\(^{160}\) In doing so, the Court rejected the interpretation that the Ninth Circuit’s panel decision in Nosal had given to the word “so” in the definition of “exceeds authorized access.”\(^{161}\) In its en banc decision, the Ninth Circuit found that too much emphasis on the word “so” was unfounded and that such an interpretation would “transform the CFAA from an anti-hacking statute into an expansive misappropriation statute.”\(^{162}\) The court stated that Congress would likely use much more straightforward language if it intended to criminalize violations of computer use restrictions.\(^{163}\) In support of this position, the court noted that in the federal trade secrets statute Congress used “common law terms for misappropriation, including ‘with intent to convert,’ ‘steals,’ ‘appropriates’ and ‘takes.’”\(^{164}\)

The court also addressed the need to interpret the term “exceeds authorized access” consistently in various subsections of the CFAA, because the term has a single definition.\(^{165}\) The government maintained that the court’s concerns about adequate notice of criminal liability were unfounded in cases brought under section 1030(a)(4) because

\(^{154}\) Id. at 860-61.
\(^{155}\) Id. at 862 (citing United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)).
\(^{156}\) Nosal IV, 676 F.3d at 862.
\(^{157}\) Id. at 860 (citing Lee v. PMSI, Inc., 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011)).
\(^{158}\) Nosal IV, 676 F.3d at 862.
\(^{159}\) Id. at 859-60.
\(^{160}\) Id. at 857-58.
\(^{161}\) Id.
\(^{162}\) Id. at 857.
\(^{163}\) Id.
\(^{164}\) Id. at 857 & n.3 (citing 18 U.S.C. § 1832 (2012)).
\(^{165}\) Nosal IV, 676 F.3d at 859.
that section punishes those who exceed authorized access “knowingly and with intent to defraud.” The court however, asserted that “exceeds authorized access” is governed by the same definition throughout the statute and that principles of statutory construction require courts to construe terms consistently for all sections of the statute. The court noted that section 1030(a)(2)(C) is the broadest provision in the CFAA, making it a crime to exceed authorized access to a computer connected to the Internet without any culpable intent. Thus, the court reasoned, a broad reading of “exceeds authorized access” proposed by the government would make every violation of a private computer use policy a federal crime.

V. CIRCUIT SPLIT

The circuit split focuses on interpretation of the terms “without authorization” and “exceeds authorized access” in the CFAA. The differences in interpretation are largely a function of how the courts view the purpose of the statute. In Nosal IV, the court made it clear that the CFAA is not a statute that should be used to punish employees who use their access to misuse information. The court rejected interpretations by circuits that have found employees liable or guilty under the CFAA for violating computer use policies or for violating a duty of loyalty.

In Nosal IV, the dissent stated that “none of the circuits that have analyzed the meaning of ‘exceeds authorized access’ as used in the Computer Fraud and Abuse Act read the statute the way the majority does.” As the dissent noted, the First, Fifth, Seventh, and Eleventh Circuits have found civil or criminal violations under the CFAA in the following situations: the employee violated a broad confidentiality agreement; the employee violated a duty of loyalty to his employer; the employee accessed information with a criminal purpose; or the employee knowingly violated an employment policy. In these cases, the courts found that it did not matter whether access itself was authorized; what mattered was the intent in accessing information, the purpose of accessing the information, or the unauthorized or unlawful use of the information. In contrast, the Ninth Circuit’s decision in Nosal IV states that the inquiry must begin with whether or not access itself was authorized or exceeded.

166 Id.
167 Id. (citing Powerex Corp. v. Reliant Energy Serv., Inc., 551 U.S. 224, 232 (2007) (“identical words and phrases within the same statute should normally be given the same meaning”)).
168 Nosal IV, 676 F.3d at 859.
169 Id.
170 Id. at 856.
171 Id. at 863 (citing United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int’l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006)).
172 Id. at 865 (Silverman, J., dissenting).
173 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001).
174 Int’l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).
175 United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).
176 United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), cert. denied, 131 S. Ct. 2166 (2011).
177 Nosal IV, 676 F.3d at 856-57.
Not only did the Ninth Circuit reject the decisions of sister circuits that read the CFAA broadly, it also clarified its holding in *Brekka*. The court makes it clear that the Ninth Circuit interprets the terms “without authorization” and “exceeds authorized access” in a literal manner and that the *Brekka* decision does not allow for interpretations that would target “misuse or misappropriation” of information. The dissent in *Nosal IV*, like other courts favoring a broad interpretation, suggested that *Brekka* should be read to punish individuals who have initial access to a computer but knowingly go beyond those limitations.

Recent decisions suggest that the narrow view is gaining momentum. Most notably, following *Nosal IV*, the Court of Appeals for the Fourth Circuit specifically adopted the Ninth Circuit’s narrow interpretation of the CFAA. In *WEC Carolina Energy Solutions v. Miller*, the court considered whether the terms “without authorization” and “exceeds authorized access” extend to violations of computer use policies or to misuse of information to which a defendant otherwise had access. The court held that an employee who downloaded an employer’s confidential information, emailed it to his personal account, and subsequently used that information in a presentation to the employer’s competitor, was not liable under the CFAA. The court agreed with the Ninth Circuit’s reasoning that “the CFAA fails to provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded.” The Fourth Circuit explicitly rejected “any interpretation that grounds CFAA liability on a cessation-of-agency theory,” the theory that an employee loses authorization or exceeds authorization when he breaches his fiduciary duty to the employer.

The Sixth Circuit also appears to agree with a narrow interpretation of the CFAA. In *Pulte Homes*, the court read the term “without authorization” narrowly, finding that a union had authorized access to the plaintiff’s phone and email, both of which were open to the public. The court cited the Ninth Circuit’s decision in *Brekka*, holding that “a person who uses a computer ‘without authorization’ has no rights limited or otherwise, to access the computer in question.” A lower court within the Sixth Circuit stated that the *Pulte Homes* decision “suggests that the Sixth Circuit would adopt the narrow view insofar as it relied heavily on the Ninth Circuit’s opinion” in *Brekka*. Several lower courts within the Sixth Circuit have adopted the narrow view.

---

178 Id. at 863 (citing Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)).
179 Id. at 864-65 (Silverman, J., dissenting).
180 Id. at 203.
181 687 F.3d 199, 201 (4th Cir. 2012).
182 Id.
183 Id. at 206.
184 See Pulte Homes, Inc. v. Laborers’ Int’l Union, 648 F.3d 295, 304 (6th Cir. 2011).
185 Id. (quoting LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).
Within the Eighth Circuit, district courts have also adopted a narrow reading of “without authorization” and “exceeds authorized access.”\(^{188}\) For example, in *Walsh Bishop Associates v. O’Brien*, the United States District Court for the District of Minnesota considered whether the CFAA imposes civil liability on employees who access information with permission but with an improper purpose.\(^{189}\) Noting that the Eighth Circuit has not yet decided this issue, the court stated that courts in Minnesota have preferred the narrow view, focusing on “the scope of access rather than misuse or misappropriation of information.”\(^{190}\) The court found that even if it considered the employer’s computer use policy which restricted the employees’ use of access, the CFAA claim failed because the employees had access to the areas in question.\(^{191}\)

Within the Second Circuit, district courts have also signaled a preference for the narrow approach.\(^{192}\) In a recent criminal case, *United States v. Aleynikov*, the United States District Court for the Southern District of New York clearly articulated its preference for the approach taken by the Ninth Circuit in *Brekka*, and ultimately, in *Nosal IV*.\(^{193}\) Notably, the *Aleynikov* court stated, “[w]hat use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place.”\(^{194}\) On appeal, the government did not raise the CFAA claim, but the Court of Appeals for the Second Circuit interpreted other federal statutes involving theft of trade secrets narrowly, suggesting that it would likely interpret the CFAA narrowly as well.\(^{195}\)

Significantly, the United States District Court for the District of New Hampshire was clearly influenced by the *Nosal IV* decision. In deciding a case involving allegations of

\(^{188}\) *See* Lewis-Burke Assocs. v. Widder, 725 F. Supp. 2d 187, 193 (D.D.C. 2010) (choosing to follow “the *Brekka* line of cases which have recently gained critical mass”); *see also* Clarity Serv., Inc. v. Barney, 698 F. Supp. 2d 1309, 1315-16 (M.D. Fla. 2010) (adopting narrow view and rejecting the reasoning in *Citrin*); ReMedPar, Inc. v. Allparts Medical, LLC, 683 F. Supp. 2d 605, 611-13 (M.D. Tenn. 2010) (agreeing with the reasoning in *Brekka* and rejecting the agency theory in *Citrin*).

\(^{189}\) 2012 U.S. Dist. LEXIS 25219 (D. Minn. Feb. 28, 2012). The court noted that the Eighth Circuit has not yet considered this question. *Id.* at *5.*

\(^{190}\) *Id.* at **5-6 (citing two 2011 District of Minnesota cases following the narrow view and a 2006 case favoring a broader approach). *See also* Sebrite Agency, Inc. v. Platt, No. 11-CV-3526 (PJS/SER) 2012 U.S. Dist. LEXIS 110262 at *6 (August 7, 2012) (noting prevalence of narrow interpretation in courts within the Eighth Circuit and that it “continues to believe that the narrower interpretation of the CFAA is more consistent with statutory text, legislative history, and the rule of lenity.”).


\(^{193}\) *Aleynikov*, 737 F. Supp. 2d at 191-94.

\(^{194}\) *Id.* at 192.

\(^{195}\) *See* United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012). The court held that stealing and transferring proprietary computer source code used in an employer’s high frequency trading system did not violate the National Stolen Property Act, because “the source code was not a ‘stolen’ ‘good’” within the meaning of the Act. *Id.* at 78. The court also held that the source code was not “related to or included in a product that is produced for or placed in interstate or foreign commerce” within the meaning of the Economic Espionage Act. *Id.* Interestingly, Mr. Aleynikov was recently arrested and charged under state law by Manhattan District Attorney Cyrus Vance, Jr. *See* Reed Albergotti, *Programmer’s Case is Matter of (Legal) Code*, WALL ST. J. Sept. 28, 2012, at C1.
exceeding authorized access under the CFAA, the court held that “an employee’s unauthorized use, disclosure, or misappropriation of data which he or she has obtained through authorized access is not conduct governed by the CFAA.” In reaching this conclusion, the court read the First Circuit Court of Appeal’s decision in EF Cultural in a limited manner. In Wentworth-Douglass Hospital v. Young & Novis Professional Association, the court stated that EF Cultural is better understood as a decision that allowed the defendants to gain “unauthorized access by circumventing ‘access restrictions’ to the website’s data,” rather than as a case that found the CFAA applied where employees had “violated a website’s ‘use restrictions.’” Rejecting the plaintiff’s argument that EF Cultural required a broad interpretation of the CFAA, the court stated that “the better (and more reasonable) interpretation of the phrase ‘exceeds authorized access’ in the CFAA is a narrow one” that does not govern conduct such as “an employee’s unauthorized use, disclosure, or misappropriation of data which he or she has obtained through authorized access.” In EF Cultural, the court’s analysis of the CFAA’s authorization terms was minimal and pre-dated cases in which courts debated the repercussions of a broad or narrow interpretation. Thus, the Wentworth-Douglass Hospital decision raises the possibility that the First Circuit could limit the implications of its decision in EF Cultural and adopt a narrow reading of the CFAA’s authorization terms, consistent with the interpretations of the Ninth and Fourth Circuits.

Thus, decisions in the First, Seventh, Fifth and Eleventh Circuits currently read the CFAA’s authorization terms broadly, although a lower court decision suggests that the First Circuit’s decision in EF Cultural could be limited and interpreted in favor of the narrow interpretation. The Ninth and Fourth Circuits have clearly and decisively adopted a narrow reading of the CFAA’s authorization terms. The Sixth Circuit has indicated its preference for a narrow reading that emphasizes access. Lower courts in the Second, Sixth and Eighth Circuits favor the narrow interpretation of authorization terms.

VI. DEFENDING THE NARROW INTERPRETATION OF “EXCEEDING AUTHORIZED ACCESS”

The Brekka and Nosal decisions provided the Ninth Circuit with ample opportunity to consider the CFAA’s language, intent and impact. Through comprehensive consideration and reconsideration of terms in the CFAA, the Ninth Circuit weighed a variety of well-reasoned arguments for broad, narrow, and nuanced readings of the terms “without authorization” and “exceeds authorized access.” While the dissent charged Chief Judge Kozinski, author of the en banc’s majority opinion, of “conjur[ing] up far-fetched hypotheticals,” and “knocking down straw men,” the majority’s decision is well-informed by the court’s extensive consideration of these issues and the potential impact of its interpretations.

197 See description of EF Cultural supra at text accompanying notes 55-59.
199 Id. at *9.
200 Nosal IV, 676 F.3d at 864, 867 (Silverman, J., dissenting).
The following section defends the Ninth Circuit’s narrow reading of the CFAA and its conclusion that the overall objective of the statute is primarily to address hacking rather than misappropriation of confidential information. The section then expands on the analysis in Nosal IV to confirm that a narrow interpretation is warranted. The plain language of the statute and rules of statutory construction are sufficient to support the narrow view. The rule of lenity, along with the requirement of sufficient notice that is inherent in due process jurisprudence are considerations that further support the narrow view. This section also considers the impact that the CFAA has on misappropriation laws, potentially displacing these laws, leading to the conclusion that a narrow interpretation of the statute prevents further unanticipated consequences. Finally, this section maintains that a narrow interpretation of the authorization terms conforms more closely to the type of harm the statute seeks to prevent.

A. The CFAA Targets Unauthorized External Hackers Rather Than Authorized Employee Insiders Who Misuse Business Information

Courts adopting the narrow view have emphasized that the CFAA sought to criminalize the type of computer abuse commonly referred to as external hacking. Examples of external hacking portrayed in the media typically glamorize hacker conduct, often implying that hackers are geniuses with the daring of James Bond. The 1986 Senate Report stated that “programs should be implemented that deflate the myth that computer crimes are glamorous, harmless pranks.” The myth associated with daring hackers still persists, however, as can be seen by the popularity of films such as “The Girl with the Dragon Tattoo.” The storyline portrays Lisbeth Salander, a tattooed computer researcher consulting for a private Swedish security company, as a heroine who uses her computer hacking prowess to combat evil forces, ultimately using her hacking skills to discover a serial killer, and execute a Robin Hood-like theft of funds from a corrupt businessman.

Real life instances of external hackers in the early days of the Internet engendered fear in the hearts of legislators, leading to amendments to correct perceived inadequacies. In 1988, Robert Morris, a graduate student from Cornell, was the first person prosecuted under the CFAA after he unleashed a ‘worm’ on the Internet that inadvertently caused

---

204 THE GIRL WITH THE DRAGON TATTOO (Columbia Pictures and Metro Goldwyn-Mayer Pictures 2011) (portraying Swedish external hacker Lisbeth Salander); see also Pollaro, supra note 5, at ¶4 (discussing portrayal of Matthew Broderick as whiz kid computer hacker in 1983 film War Games in which the hacker’s conduct led United States to brink of nuclear war with the Soviet Union).
205 She keeps the money for herself but it nearly seems like appropriate karma in light of how the legal system has treated her so unfairly.
206 See Kerr, Vagueness Challenges, supra note 35, at 1563.
many computers to shut down. The media conveyed a larger-than-life depiction of the monetary impact of Morris’s hacking. In 1988, the impact of the Morris worm was primarily on large institutions because home computing was in its infancy. The Court of Appeals for the Second Circuit found that Morris had sufficient intent to violate section 1030 (a)(5)(A) of the CFAA when he inserted the worm onto a computer that he was authorized to access while knowing that it would invade other computers to which he was “without authorization.” Morris’s punishment was light, however, and MIT seemingly held no lasting animosity towards him because he later became a tenured member of the faculty there.

The CFAA continues to play an important role in cases involving computer hacking. In 2010, external hacker Albert Gonzalez was charged with violating the CFAA in a credit and debit card hacking of major proportions. It is the largest known identity fraud case in U.S. history, earning T.J. Maxx the nickname T.J. Haxx, and the hacker twenty years in prison. The same year, Gonzalez was indicted for theft of credit card information from Heartland Payment Systems, information he used to create counterfeit credit cards. Another well-known external hacker was sued civilly under the CFAA in 2011. Twenty-one year old George “Geohotz” Hotz hacked Sony’s PlayStation 3 game console. Hotz was also well-known for “jailbreaking” Apple’s iPad and iPhone, so that the devices could be used with multiple non-approved wireless carriers.

While external hacking is a clear example of acting “without authorization” under the CFAA, it is less clear what Congress envisioned in prohibiting an individual from “exceeding authorized access.” The narrow interpretation of the CFAA suggests that the distinction between the terms separates external hackers from internal hackers. Thus, an internal hacker might be an employee who accesses his workplace computer system with authorization but then proceeds to exceed authorized access by using someone else’s username and password to access material he is not otherwise authorized to view. For example, an internal hacker might try to access salary information of other employees to

---

208 See Dierks, supra note 202, at 317 (discussing damage estimates of $97 million when actual damage was closer to $150,000 regarding Robert Morris’s 1988 hacking); see also United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (convicting Morris of violating CFAA for intentionally unleashing a worm on the early Internet that caused numerous institutional systems to cease functioning).
210 Morris, 928 F.2d at 507, 511.
211 See 5 Old School Hackers, Where They Are Now, Wikibon Blog, http://wikibon.org/blog/5-old-school-hackers-where-are-they-now/ (discussing Robert Morris now a professor at MIT).
213 Id.
increase his bargaining power for a raise.\textsuperscript{216} An internal hacker could also be an employee who misappropriates confidential information provided that he used some unauthorized method to gain access to the information. Although courts have not used the term “code-based authorization,” this term best captures the type of permission-based access that underlies the CFAA’s distinction between external and internal hacking.\textsuperscript{217} Thus authorization is best viewed in terms of code-based access, a concept that the Ninth Circuit endorses when it refers to “exceeding authorized access” as “circumvention of technological barriers.”\textsuperscript{218}

\begin{center}
B. Rules of Statutory Construction Support a Narrow Reading
\end{center}

Courts that have adopted the narrow reading of the CFAA have followed a consistent method of analysis, relying primarily on the plain language of the statute and the rule of lenity.\textsuperscript{219} In analyzing the plain meaning of the statute, courts have sought to construe provisions in a manner that will not violate other cardinal canons of statutory construction including: avoidance of an interpretation that would render some provisions superfluous or create absurd results; interpreting provisions that apply to criminal and civil sanctions in the same manner; avoiding interpretations that create culpability because of lack of notice of its status as a crime, ultimately resulting in judicial determination that the provision is constitutionally deficient as it is void for vagueness. Finally, the rule of lenity advocates interpreting criminal statutes that contain an ambiguous phrase in a manner that is more lenient rather than draconian in its consequences to defendants.

\begin{center}
1. Plain Meaning
\end{center}

Under the narrow view, courts present a strong case that the plain language meaning of the statute prohibits improper access to information, not improper purpose in accessing information or improper use of information.\textsuperscript{220} The “fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their

\textsuperscript{216} See Chris Conetsky, Internal hacking poses silent threat for companies, BUSINESS RECORD, (Dec. 5, 2009), http://businessrecord.com/main.asp?SectionID=5&SubSectionID=9&ArticleID=9201&TM=25414.8 (last visited May 27, 2012) (noting internal hacking occurs when employees access data to which they are not entitled, and use it for purposes of their own gain including selling company secrets).

\textsuperscript{217} See Kerr, Cybercrime’s Scope, supra note 4, at 1655 (noting authorized user who exceeds code-based access by use of another’s user name and password has engaged in fraud in the factum, and such voids the authorization).

\textsuperscript{218} Nosal IV, 676 F.3d at 863-64.


\textsuperscript{220} Nosal IV, 676 F.3d at 863 (holding that “the phrase ‘exceeds authorized access’ in the CFAA does not extend to use restrictions’); Orbit One Comm’ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (“The CFAA expressly prohibits improper ‘access’ of computer information. It does not prohibit misuse or misappropriation.”).
The phrase “without authorization” is not defined in the CFAA. Thus, the word “authorization” must be read in accordance with its ordinary meaning; that is, in accordance with ordinary dictionary definitions such as “permission or power granted by an authority” or “the state of being authorized” or “entitled.” In an ordinary employment situation involving computer use, the employer grants an employee authorization to access a company computer, providing the employee with a user name and password for access. The grant of this code-based permission is generally determinative of whether an employee has authorized access. In evaluating the CFAA, some courts have seen no ambiguity in the phrase “without authorization” and refused to consider further extrinsic evidence to elucidate the language.

“Exceeding authorized access” has proved to be the more frequently litigated term, even though the statute provides a definition. To “exceed authorized access” means “to access a computer with authorization and to use such access to obtain information in the computer that the accesser is not entitled so to obtain and alter.” A common sense reading of the plain language of the definition allows: that the individual has initial authorization to access the computer, but then the authorized accesser uses that access to go beyond the accesser’s authorization to obtain information or data that the individual is not entitled (or authorized) to obtain and alter.

---

221 Perrin v. United States, 444 U.S. 37, 42 (1979) (citing Burns v. Alcala, 420 U.S. 575, 580-81 (1975)). The Court in Perrin was interpreting language of a federal criminal statute that, like the CFAA, created a federal cause of action for traditional state or local crimes where such had an interstate nexus. See also Dowling v. United States, 473 U.S. 207, 213 (1985) (noting that federal crimes are “solely creatures of statute” and statutory construction begins with the ordinary meaning of the language).


223 See LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132-35 (9th Cir. 2009); see also United States v. Aleynikov, 737 F. Supp. 2d 173, 191-92 (S.D.N.Y. 2010) (“a person who ‘exceeds authorized access’ has permission to access the computer, but not the particular information on the computer that is at issue.”).

224 Nosal IV, 676 F.3d at 856-57.

225 It is possible that in some very basic employment situations an employer could provide a computer without a user name and password and allow usage based upon employee presence rather than organizing authorization through the more secure method of providing the employee an individual user name and password. However, more commonly, especially at sophisticated institutions, there are likely to be various layers of access granted within a company, based upon the information that an employee needs to be able to access in order to properly perform the job. Those who run the system and/or run the company tend to have the broadest, often termed administrative privileges. See generally Chung, supra note 222, at 247-56 (2010) (discussing computer security model of CFAA interpretation including access control lists).

226 See Lockheed Martin Corp. v. Speed, No., 2006 U.S. Dist. LEXIS 53108, at *15 (M.D. FL. Aug. 1, 2006) (explicitly rejecting the agency-based approach and finding the plain language “without authorization” clear without the need for consideration of extrinsic legislative history); see also Field, supra note 71, at 821 & n.6 (discussing Lockheed and other district court cases that refused to adopt the employer-friendly agency-based approach to “without authorization” or “exceeding authorized access”).

227 See DOJ IP Manual, supra note 13, at 12, 14 (noting most litigated issue about “exceeding authorized access” is whether exceeded by accessing for improper purpose).


of the clearest explanations of the difference between “without authorization” and “exceeds authorized access”:

The CFAA targets access “without authorization” in six separate offenses (§ § 1030(a)(1), (a)(2), (a)(3), (a)(4), (a)(5)(A)(iii), only three of which also reach persons “exceeding authorized access” (§ § 1030 (a)(1), (a)(2), (a)(4). Thus, it is plain from the outset that Congress singled out two groups of accessers, those “without authorization” – or those below authorization, meaning those having no permission to access whatsoever – typically outsiders, as well as insiders that are not permitted any computer access) and those exceeding authorization (or those above authorization, meaning those that go beyond the permitted access granted to them – typically insiders exceeding whatever access is permitted to them).

The narrow interpretation of authorization terms has the advantage of an objective assessment of whether the employee had permission to access the information in question. Broad interpretations of the authorization terms rely on an employee’s subjective intent when accessing confidential information. There is nothing in the statute that links authorization to intent. One court noted that the analysis in Citrin would suggest that an employee’s authorization status could shift throughout his employment, depending on his state of mind at the time of access. The court stated that “Congress could not have intended a person’s criminal and civil liability to be so fluid, turning merely on whether a person’s interests were adverse to the interests of an entity authorizing the person’s access.” It is true that section 1030(a)(4) hinges on a defendant’s criminal or fraudulent intent, but the intent requirement cannot be imputed to other sections of the CFAA that use the terms “without authorization” and “exceeds authorized access.” Moreover, as the Ninth Circuit discusses in Nosal IV, the CFAA provides a single definition of “exceeds authorized access” and giving the term different meanings in different sections violates the principle of statutory construction that

---


232 See LVRC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (“No language in the CFAA supports [the] argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer’s interest.”).


234 Id. at 194 (citations omitted).
“identical words and phrases within the same statute should normally be given the same meaning.”

The narrow approach has the further advantage of giving a sensible construction to both “without authorization” and “exceeds authorized access.” Courts adopting the broad view make no attempt to recognize that the terms must have distinct meanings. It is hardly likely that Congress would trouble itself to make the “paper-thin” distinction that the Seventh Circuit mentions in Citrin. Courts have criticized the reasoning courts adopted in cases such as Shurgard and Citrin because such courts “overlook[ ] the distinction between, and thereby conflate [ ], the ‘without authorization’ and ‘exceeds authorized access’ prongs of the statute.” In terms of statutory construction, the Supreme Court has noted that Congress “does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions – it does not, … hide elephants in mouseholes.” A broad interpretation of the authorization terms would be just such a miscalculated storage scheme.

2. Legislative History

There is little in the legislative history that speaks directly to the various interpretations that the courts have given the terms “without authorization” and “exceeds authorized access.” Nevertheless, as noted in Nosal IV, there is some evidence in the statute’s history that supports a narrow reading of “exceeds authorized authority.” An earlier version of the CFAA defined “exceeds authorized access” as “having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.” That language was removed and replaced by the current phrase and definition in section 1030(e)(6). The Senate Report states that the change “removes from the sweep of the statute one of the murkier grounds of liability, under which a[n] . . . employee’s access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances . . .”

In a more general sense, the legislative history gives little support to the theory that disloyal employees should be targeted under the CFAA. In fact, even though the legislative history shows concern for the security of information available to government employees, the Senate Report accompanying the 1986 amendment instructs that the “federal computer crime statute not be so broad as to create a risk that government

235 Nosal IV, 676 F.3d at 859 (citing Powerex Corp. v. Reliant Energy Serv., Inc., 551 U.S. 224, 232 (2007)).
236 See Brekka, 581 F.3d at 1133.
237 See Int’l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (stating that the difference between “without authorization” and “exceeds authorized access” is “paper thin” but “not quite invisible”).
240 See, e.g., Kerr, Cybercrime’s Scope, supra note 4, at 1616 (noting difficulties regarding meanings of access and authorization legislatures never resolved).
employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct." The legislative intent was clear that there was a preference for administrative rather than criminal sanctions in cases where such an individual exceeded access.

The Senate Report on the 1986 amendments to the CFAA also indicates that Congress intended private companies to police their own security. Such intent is contrary to a broad reading that would criminalize an array of employee behavior. The Report references its agreement with an ABA Task Force Report on Computer Crime that supported the enactment of the federal computer crime statute but also believed in the ability of the “potential targets of such conduct” to prevent the crimes themselves. Both the ABA Report and the Judiciary Committee supported the idea that private industry and individual users should take “primary responsibility for controlling the incidence of computer crime” by use of more effective self-protection.

Proponents of the broad interpretation of the CFAA cite the numerous amendments to the statute expanding liability as support for Congress’s intent to broaden the CFAA’s scope and reach. Both the 1994 amendment providing a private cause of action and the 1996 amendment which broadened the definition of “protected computers,” certainly gave the CFAA greater scope. These amendments, however, are more appropriately read to allow private employers to recover for damages related to computer misconduct involving hacking rather than to criminalize misappropriation of confidential information.

3. Void for Vagueness and the Rule of Lenity

The narrow interpretation of the terms “without authorization” and “exceeds authorized access” under the CFAA gains additional support from rules of construction such as the rule of lenity and the void for vagueness doctrine. The rule of lenity has been a part of American jurisprudence since 1820 when the United States Supreme Court refused to enlarge on the coverage of the first federal criminal statute. The rule requires that any ambiguity in a criminal statute be resolved in favor of defendants. The purpose of the rule is to ensure notice and legislative supremacy. The notice theory prevents criminals from unforeseen interpretations of statutes that they could not reasonably have anticipated, and further, it ensures legislative supremacy guaranteeing that courts will not exceed the legislative intent behind the statute. A vague law may authorize and even encourage arbitrary and discriminatory enforcement.

---

244 S. REP. No. 99-432, supra note 203, at 7.
245 S. REP. No. 99-432, supra note 203, at 3.
246 S. REP. No. 99-432, supra note 203, at 3.
247 See, e.g., NCMIC Finance Corp. v. Artino, 638 F. Supp. 2d 1042, 1058-59 (S.D. Iowa 2009) (citing the private cause of action and the “protected computer” definition as support for the broad view); Guest-Tek Interactive Entm’t, Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009) (citing “the consistent amendments that Congress has enacted to broaden [the CFAA’s] application”).
250 Id. at 886.
concerns, the doctrine requires that courts construe criminal laws narrowly to cure the vagueness.\textsuperscript{252}

In the recent unrelated case of \textit{Skilling v. United States} involving the former Enron officer, the Supreme Court reaffirmed the requirements of the void-for-vagueness doctrine, stating that “a penal statute [must] define the criminal offense [1] with sufficient definiteness that ordinary people can understand what conduct is prohibited and [2] in a manner that does not encourage arbitrary and discriminatory enforcement.”\textsuperscript{253} Thus, in the \textit{Skilling} case, the Court mentioned that the rule of lenity provided additional support for its decision to reduce the scope of a criminal statute to bribery and kickback schemes where there was ambiguity relating to Skilling’s purported scheme to deprive another of intangible honest services.\textsuperscript{254}

It is clear that the rule of lenity and the void-for-vagueness doctrines both serve the purpose of ensuring adequate and fair notice to potential defendants charged with violations of the CFAA. A broad interpretation of the CFAA may criminalize behavior that is prohibited only in an employment policy, an employment agreement, or even a website’s Terms of Service. As the court points out in \textit{Nosal IV}, employees and consumers are usually unaware of the contents and prohibitions contained in these cumbersome agreements.\textsuperscript{255}

Both the rule of lenity and the void-for-vagueness doctrine call for a narrow interpretation of criminal conduct in the face of ambiguity. The rule of lenity is not used independently to reach a conclusion, but it adds that extra bit of glue to hold the whole structure of support for a judicial interpretation together. As one commentator noted, the rule of lenity provides a “tiebreaker” to resolve the circuit split on the interpretation of authorization under the CFAA.\textsuperscript{256} Similarly, in \textit{Brekka}, the court stated, “[n]othing in the CFAA suggests that a defendant’s liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer . . . . It would be improper to interpret a criminal statute in such an unexpected manner.”\textsuperscript{257}

The established canon of statutory construction lends support for a narrow over a broad interpretation.\textsuperscript{258} In \textit{Nosal IV}, the court anticipates that a broad reading of the CFAA

\textsuperscript{252} See Kerr, \textit{Vagueness Challenges}, supra note 35, at 1573 & n.91 (citing City of Chicago v. Morales, 527 U.S. 41, 64, 92, 112 (1999)).

\textsuperscript{253} See \textit{Kerr, Vagueness Challenges}, supra note 35, at 1573 & n.91 (citing City of Chicago v. Morales, 527 U.S. 41, 64, 92, 112 (1999)).


\textsuperscript{255} Skilling, 130 S. Ct. at 2906. Justice Ginsburg, writing for the majority, cautioned against extending ‘honest services’ beyond its core meaning for it “would encounter a vagueness shoal.” \textit{Id.} at 2907.


\textsuperscript{259} See Booms, supra note 10, at 555; Kerr, \textit{Vagueness Challenges}, supra note 35, at 1587 (criticizing broad agency theory of authorization because it would turn millions of employees into criminals, giving the government power to arrest almost anyone who had a computer at work).
could lead to absurd results.\textsuperscript{259} The court provides an example of an employee who “spends six hours tending his Farmville stable on his work computer.”\textsuperscript{260} Although the employee has full access to the computer, he arguably exceeds authorized access and defrauds the employer by depriving the employer of six hours of work. According to the court, an aggressive prosecutor could charge this employee under a broad reading of the CFAA.\textsuperscript{261}

\textit{C. A Narrow Interpretation Prevents Intrusion on Misappropriation Laws}

In addition to cogent arguments based on plain language analysis and canons of statutory construction, courts must be mindful that employees’ disloyal behavior is already addressed by a cohort of other federal and state laws. In \textit{Nosal IV}, the court stated that Congress gave no indication that it intended the CFAA to function as a misappropriation statute and that Congress would certainly have used plainer language if it so intended.\textsuperscript{262} The court also stated that contract and tort law traditionally have been the domain of misappropriation law.\textsuperscript{263} Courts that have explored the limits of the CFAA in the employment context merely have touched on these concerns. A broad interpretation of the CFAA has the unintended effect of allowing plaintiffs to make a case for trade secret theft more easily and also of disturbing the balance between federal and state jurisdiction over such claims.\textsuperscript{264} A narrow reading of the CFAA would avoid such federalism problems.\textsuperscript{265}

Reading the CFAA narrowly is not a question of letting underhanded and dishonest employees go unpunished, but the statute should not criminalize acts that heretofore were the province of contract and tort law. Plaintiffs and prosecutors are not without other means of pursuing these disloyal employees. In civil cases, an employer might allege claims involving breach of contract, tortious interference with contract and prospective business relations, or misappropriation of trade secrets in violation of state laws. In criminal cases, defendants may be charged with mail fraud and trade secret theft under the Electronic Espionage Act (EEA), as Nosal was.\textsuperscript{266}

In several cases, employers have sought relief under the CFAA for claims that involve theft of trade secrets.\textsuperscript{267} The fact that the EEA does not allow a private right of action for trade secret theft makes it highly unlikely that Congress intended to provide such a remedy through the CFAA. A broad interpretation of the CFAA allows employers to clear the authorization hurdle easily and succeed on claims with much less effort than the

\begin{itemize}
\item \textsuperscript{259} \textit{Nosal IV}, 676 F.3d at 863 (Chief Judge Kozinski noted that the “narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere” [referring to the Economic Espionage Act]).
\item \textsuperscript{260} \textit{Nosal IV}, 676 F.3d at 860 & n.7.
\item \textsuperscript{261} \textit{Id}.
\item \textsuperscript{262} \textit{Id.} at 857 & n.3.
\item \textsuperscript{263} \textit{Id.} at 860.
\item \textsuperscript{264} \textit{See} Brenton, \textit{supra} note 9, at 430-31.
\item \textsuperscript{265} \textit{See} Brenton \textit{supra} note 9, at 454-55, 460-61.
\item \textsuperscript{266} \textit{Nosal IV}, 676 F.3d at 856.
\item \textsuperscript{267} \textit{See}, \textit{e.g.}, \textit{Nosal IV}, 676 F.3d at 863 (refusing to hold CFAA covers misappropriation of trade secrets).
\end{itemize}
EEA or a state trade secret theft statutes demand. An employer can be awarded damages under the CFAA merely by proving that the information was on a computer, that defendants obtained that information through unauthorized access or access exceeding existing authorization, and that the employer has suffered damage or loss. The elements required to prove a case of trade secret theft – the information was not generally available, it gained value from secrecy, and reasonable steps were taken to protect the information – need not be proven. Thus, one commentator states that “[s]ince the evidentiary elements of proof of a CFAA . . . claim are far lower than in a traditional trade secret misappropriation claim, there exists a danger that the substantive law of trade secrets will be eclipsed by CFAA litigation.”

D. A Narrow Interpretation Conforms with the Type of Harm the Statute Anticipates

The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” “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.”

Like the dispute over authorization terms, courts differ in whether or not to interpret the damage and loss provisions broadly or narrowly. Several courts have stated that misappropriation of confidential information alone does not satisfy the damage and loss provisions. Courts that follow the broad reading of the statute conclude that accessing

---

268 See Brenton, supra note 9, at 440.
269 See Brenton, supra note 9, at 438-89.
270 See Brenton, supra note 9 at 443-44 (citing elements of trade secret misappropriation at Unif. Trade Secrets Act § 1(2) (1985)). Brenton also deprecates the use of the CFAA in trade secret theft cases because it upset the balance between employers and employees, in terms of the cost of protecting business information and employee mobility. Brenton, supra note 6, at 450. According to Brenton, the broad interpretation of the CFAA, represented by cases such as Shurgard and Int’l Airport Ctrs, gives the employer the “equivalent of a nuclear weapon.” Id. See also Reder & O’Brien supra note 7, at 389 (discussing elements of proof in a trade secret claim).
271 See Brenton, supra note 9, at 440.
275 See id. at *22 (“compromise or decrease in the competitive value of . . . confidential information does not satisfy the damage requirement . . . .); see also Lockheed Martin Corp. v. Speed, 2006 U.S. Dist. LEXIS 53108, at *26 (M.D. Fl. Aug. 1, 2006) (holding that copying confidential information is not damage under the CFAA). See generally Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 937 (W.D. Tenn. 2008) (agreeing with the narrow view generally but finding that “intentionally rendering a computer system less secure should be considered ‘damage’ under § 1030(a)(5)(A) (2012), even when no data, program, or system is damaged or destroyed”).
and disclosing trade secrets can constitute an impairment to the integrity of data or information. 276

The language in these sections indicates the type of harm caused by hacking or altering information on a system, and not loss associated with disloyal employment practices or theft of trade secrets. 277 The language of the statute reasonably suggests that “damage” would include “the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or ‘diminution in the completeness or usability of the data on a computer system.’” 278 Thus, for example, the Court of Appeals for the Sixth Circuit found that a barrage of emails and phone calls that interrupted or weakened a company’s computer system, limiting its ability to receive calls or email, would be “damage” within the meaning of the statute. 279 Similarly, courts have read the term “loss” narrowly to include costs associated with interruption of service and investigation or response to computer damage or intrusion. 280

VII. ANALYSIS AND RECOMMENDATIONS

The Ninth Circuit’s decision in Nosal IV, followed by the Fourth Circuit’s decision in WEC Carolina Energy Solutions LLC v. Miller, marks a decided shift towards a narrow reading of the CFAA. Under this view, employees would be prosecuted or held liable under the Act only when they accessed information without any permission or by circumventing code based restrictions. Thus, an employee who uses a co-worker’s password to access information he is not personally entitled to access would exceed authorized access under the CFAA. An employee who downloads information to his private computer after resigning or being terminated would violate the CFAA for

---

276 See, e.g., Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000); George S. May Int’l Co. v. Hostetler, 2004 U.S. Dist. LEXIS 9740, at **10-12 (N.D. Ill. May 28, 2004) (finding that infringement of copyrighted material taken from computer qualifies as impairment of integrity of data under the CFAA). In EF Cultural Travel BV v. Explorica, Inc., the Court of Appeals for the First Circuit adopted a broad reading of the damage and loss provisions under the CFAA. 274 F.3d 577, 585 (1st Cir. 2001). The decision suggests that “any loss is compensable” provided the plaintiff meets the statutory threshold. Id.

277 See generally Warner, supra note 75, at 1-13, 18-19 (noting that CFAA is aimed at hackers and it provides complementary claim to trade secret claims as easier to prove).


279 Pulte Homes, Inc. v. Laborers’ Int’l Union, 648 F.3d 295, 301-02 (6th Cir. 2011). Even though the plaintiffs were able to show CFAA “damage,” the court dismissed the CFAA claim because it construed “without authorization” narrowly to find that the defendants had authorized access to the system. Id. at 304. In Ajuba Int’l, LLC v. Saharia, 2012 U.S. Dist. LEXIS 66991, at *31 (E.D. Mich. May 14, 2010), also a federal district court within the Sixth Circuit, the court predicted that that the Sixth Circuit would adopt a narrow interpretation of authorization terms in the context of an employment dispute under the CFAA because of Pulte’s narrow reading of the term “without authorization” and that courts reliance upon the Ninth Circuit’s decision in Brekka.

280 See Bashaw v. Johnson, 2012 U.S. Dist. LEXIS 64617 (D. Kan. May 9, 2012) (stating that “the majority of courts have construed the term ‘loss’ to include only two types of injury – costs incurred (such as lost revenues) because the computer’s service was interrupted and costs to investigate and respond to computer intrusion or damage.”); see also Trademotion, LLC v. Marketeiq, Inc., 2012 U.S. Dist. LEXIS 28032, at *14-16 (Feb. 14, 2012) (noting the split in authority on whether “all losses . . . [must] be incurred due to an interruption of service”).
accessing information without authorization. In contrast, an employee who accesses information while still employed, but with the intention of using such information to compete with his employer does not violate the CFAA, although he could certainly be held accountable under other theories.

As the number of courts adopting a narrow interpretation of the CFAA is growing, employers in an increasing number of jurisdictions should be aware that they may not be able to gain additional protection through this statute and will have to use traditional avenues such as tort and contract law to pursue disloyal employees who breach computer use policies or confidentiality agreements. Moreover, at least one court has cautioned that “simply denominating limitations as ‘access restrictions’ does not convert what is otherwise a use policy into an access restriction.” Thus, employers should impose code-based access restrictions to the greatest extent possible.

The clarity and predictability of the narrow interpretation as outlined in Nosal IV and WEC provide an opportunity for courts to alert employers to the limitations of the CFAA. As courts have the opportunity to consider or reconsider the scope of the CFAA, they should be convinced that the narrow view is the better reasoned course. While the narrow interpretation of the CFAA takes away a legal weapon from employers, the broad interpretation gives an unfair advantage to employers. Employers would wield a heavy stick over potentially departing employees if they could inform prosecutors of CFAA violations based upon violations of workplace policies that are subject to change at the employers’ discretion. Moreover, the employer’s ability to change policies at will raises due process concerns about an employee’s ability to know when conduct might subject him to criminal prosecution.

If the United States Supreme Court granted certiorari to resolve the current circuit split, it would most likely find that the narrow view is the better approach. While a criminal case such as Nosal might present more compelling facts for Supreme Court review than a civil case, all courts addressing the scope of the CFAA have recognized that the definition of the authorization terms must be the same in both criminal and civil cases. Justice Scalia has stated that the Court recognizes that “when the same violation of law is made subject to both a civil or criminal penalty and a private claim for the injury inflicted . . . the language defining the violation is to be given one meaning (a narrow one).” The textualists on the Court would undoubtedly underscore the importance of giving distinct meaning to the two terms “without authorization” and “exceeds authorized access.” Consequently, the Court would most likely conclude that the reasoning that supports a broad interpretation of the terms is flawed because it fails to account for any meaningful distinction between the terms. Justices who construe statutes more liberally would still be convinced that the terms must have distinct meanings. Moreover, a narrow interpretation of the statute is more in line with congressional intent to punish hacking and

---


283 See id. at 15 (discussing textualism approach as beginning and ending with “what the text says and fairly implies.”).
circumvention of technical barriers. Even though the statute has expanded over the years, the Court would have difficulty finding any evidence that Congress intended to allow the CFAA to serve as a statute that punishes misappropriation of confidential information, breach of employment agreements or terms of service.

Congress could amend the CFAA to clarify the scope of the Act. At this writing, a proposed amendment for increasing penalties under the CFAA would provide language that narrows the meaning of “exceeds authorized access.” The amendment would make it clear that exceeding authorized access:

- does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.  

If Congress intended to criminalize a broader array of employee misconduct and intended employers to recover under the CFAA for various acts of disloyalty associated with computer use, a more substantial amendment addressing these concerns is required. If Congress intended to criminalize breach of confidentiality agreements, employment contracts and terms of service, merely by virtue of the fact that a computer was involved in the wrongdoing, surely it would provide more guidance. Many of the cases involving disloyal employees that have been brought under the CFAA are similar to cases involving theft of commercial trade secrets, a crime that is already addressed by the EEA. It would seem that Congress would have amended the EEA to provide a private cause of action if it intended to provide relief for employers in a federal case.

Whether the different approaches to the CFAA are decided by the courts or Congress, the realities of the scope of computer use in today’s society must be considered. It is increasingly difficult to separate business and non-business access to information. A broad interpretation of the authorization terms under the CFAA is especially problematic in the current environment where computer use is no longer grounded in a stationary computer at the workplace. Employees are tethered to their iPhones, Blackberries, iPads and netbooks, using them for both business and pleasure wherever they are and whatever else they are doing. They are multitasking, clicking through terms of service without reading them, and are, for the most part, disinterested in reading the minutiae of workplace computer use policies or terms of service. Courts that follow the broad

---

approach to interpreting authorization must bear in mind that such an approach can have harsh results. As the Ninth Circuit stated in *Nosal IV*, courts that have adopted the broad reading have “looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute’s unitary definition of ‘exceeds authorized access.’”

CONCLUSION

In *Nosal IV*, the Ninth Circuit adopts a reading of authorization that is based on “circumvention of technological barriers.” This interpretation is well-supported by the plain meaning of the statute and rules of statutory construction. Further amendment to the statute could clarify the meaning of the terms “without authorization” and “exceeds authorized access.” The narrow interpretation of these terms, however, as expressed in the Ninth Circuit’s decision in *Nosal IV*, has the advantage of providing courts with an objective manner in which to determine whether an employee is “without authorization” or has “exceeded authorized access.” Broad interpretations, by contrast, require courts to assess numerous, amorphous variables such as the terms of employment policies or agreements, the extent of the employee’s knowledge of such terms, and the employee’s purpose or intent in accessing the information. Such variables generate inconsistencies and uncertainties. Proponents of the narrow view are not sympathetic to disloyal employees. Rather, they seek to avoid the unintended deleterious consequences of a broad reading of the CFAA, most notably criminalizing innocuous behavior while displacing and disrupting contract and tort laws. The CFAA serves an important function in punishing both external and internal hacking and allowing private parties to recover for damages associated with such behavior. It is best to limit its function to this type of misconduct and leave the misappropriation of confidential information to laws specifically tailored to that end.

---

285 *Nosal IV*, 676 F.3d at 856.