EXCEEDING AUTHORIZED ACCESS IN THE WORKPLACE: PROSECUTING DISLOYAL CONDUCT UNDER THE COMPUTER FRAUD AND ABUSE ACT

by

Stephanie Greene*

&

Christine Neylon O'Brien**

*Associate Professor, Business Law, Carroll School of Management, Boston College

**Professor, Business Law, Carroll School of Management, Boston College

Contact information:

Stephanie Greene
stephanie.greene@bc.edu
Tel. (617) 552-1169

Christine N. O'Brien
obriencq@bc.edu
Tel. (617) 552-0413

Mailing Address:
Business Law, Carroll School of Management
Fulton 420
140 Commonwealth Avenue
Chestnut Hill MA 02467-3808
Fax: (617) 552-0414

EXCEEDING AUTHORIZED ACCESS IN THE WORKPLACE: PROSECUTING DISLOYAL CONDUCT UNDER THE COMPUTER FRAUD AND ABUSE ACT

Abstract

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. 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. 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.

This article focuses on the variety of ways courts construe 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 acts 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.*

I.INTRODUCTION

Computers have introduced new distractions and new temptations into the workplace. Employees may use work time to shop, socialize or gamble on an employer's computer even though such behavior is prohibited by the employer's computer use policy or by employment agreement. 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 policy has blurred.[1] What repercussions should an employee suffer if he violates an employer's computer use policy? Some violations may be de minimis whereas others might pose substantial threats to the employer – such as harm to its reputation or exposure of confidential information. In the most extreme cases, employees may use an employer's computer to commit crimes. Thus, misuse of an employer's computer encompasses a broad spectrum of behavior from the lazy employee who squanders time at the computer to a scheming criminal.

[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).

Issues of employee disloyalty have traditionally been the province of contract and tort law,[2] with employers suing disloyal employees for misappropriation of trade secrets, conversion, unfair competition, and tortious interference with a business expectancy.[3] 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 the business keeps secret in order to maintain its economic advantage. [4] The Economic Espionage Act (EEA) of 1996 makes theft or misappropriation of trade secrets related to a product in foreign or interstate commerce a federal crime.[5] The EEA, however, contains no private right of action. [6]

The Computer Fraud and Abuse Act (CFAA), however, does provide a private right of action and has increasingly been used to sue employees whose misconduct or disloyalty has some relationship with a computer.[7] Numerous cases involving misappropriation of confidential information have been brought under the CFAA.[8] 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.[9]

---

[2] *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, Int'l Bhd. of Elec. Workers, (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).

[3] *See, e.g.*, Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1122 (W.D. Wash. 2000) (in addition to violations of the CFAA, plaintiff's complaint alleged misappropriation of trade secrets, conversion, unfair competition, and tortious interference with a business expectancy).

[4] *See* Margo E. K. Reder & Christine Neylon O'Brien, *Managing the Risk of Trade Secret Loss Due to Job Mobility in an Innovation Economy with the Theory of Inevitable Disclosure*, 12 J. HIGH TECH. L. 373, 382 (2012) (defining the law of trade secret), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014051, http://www.jhtl.org/docs/pdf/Reder%20and%20O%27Brien%20-%20Managing%20the%20Risk%20of%20Trade%20Secret%20Loss.pdf (last visited May 28, 2012); Uniform Trade Secrets Act sections 1-12 (amended 1985), 14 U.L.A. 529-659 (Supp. 2010) [hereinafter UTSA].

[5] *See* 18 U.S.C. §§1831 et seq. (2008).

[6] *See* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L.TECH. & POL'Y 429, at 353 & n.173 (2009**)** (noting absence of private cause of action**).**

[7] *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).

[8] *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, §2102 (a), 98 Stat. 2190, 2190-92. The Computer Fraud and Abuse Act is the name of the 1986 amendment to 18 U.S.C. § 1030, Pub. L. No. 99-474, 100 Stat. 1213 (1986); *see* Booms, *supra* note 7 at 557-58 (discussing courts that have adopted broad view that employee misuse vitiates authorization).

[9] *See generally* Garrett Urban, *Causing Damage without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1376-79 (2011) (discussing cases applying agency and contract theories to exceeding authorized access under CFAA).

Increasingly, the Department of Justice has also sought to prosecute crimes involving employees who violate employment policies or agreements under the CFAA.[10] 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.[11] As the number of such cases have grown, the courts have struggled to determine the extent to which the CFAA is an appropriate vehicle for holding disloyal employees accountable in both the civil and criminal context.

In 2012, the Court of Appeals for the Ninth Circuit issued an en banc decision that emphasized that the CFAA is "an anti-hacking statute" not "an expansive misappropriation statute."[12] In *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.[13] The Ninth Circuit stands alone among the circuit courts of appeal in interpreting the CFAA so narrowly.[14] Other circuit courts of appeal thus far have read the statute more broadly, finding employees guilty 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."[15]

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 Act for a variety of computer-related misconduct.[16] Chief Judge Kozinski's savvy opinion in *United States v. Nosal*, however, marshals the arguments that several district courts and noted

---

[10] *See* Office of Legal Education, Executive Office for United States Attorneys, U.S. Dep't of Justice, Computer Crime and Intellectual Property Section, Criminal Division, PROSECUTING INTELLECTUAL PROPERTY CRIMES 22-23 (3d ed. Sept. 2006) [hereinafter DOJ IP Manual] (reasoning that "criminal sanctions are often warranted to punish and deter the most egregious violators" and detailing strategies for prosecution), *available at* http://www.lb5.uscourts.gov/ArchivedURLs/Files/09-20074%281%29.pdf (last visited May 19, 2012).

[11] *See* Brenton, *supra* note 6, 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).

[12] United States v. Nosal, No. 10-10038, 2012 U.S. App. LEXIS 7151 at *7 (9th Cir. April 10, 2012) (*Nosal IV*).

[13] *Id.*

[14] *Id*. at **23-24 ("respectfully declin[ing] to follow our sister circuits….").

[15] *See* United States v. Rodriguez, 628 F. 3d 1258, 1263-64 (11th Cir. 2010) (CFAA violated due to employer policy breach); 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); Int'l Airport Centrs, LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (CFAA violated for unlawful access when agency relationship terminated for breach employment contract and breach of duty of loyalty); 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). The Second Circuit's stance on CFAA cases is possibly in flux at this time. *Compare* United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (finding CFAA violation for unauthorized access) *with* United States v. Aleynikov, 2012 U.S. App. LEXIS 7439, at *7 (2d Cir. April 11, 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"). *See infra* Part V.

[16] *See* United States v. Rodriguez, 628 F.3d 1258, (11th Cir. 2010) (CFAA violated when employee viewed information for a nonbusiness purpose); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (CFAA violated when employee used information with purpose of committing fraud); 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); 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).

scholars have made against broad use of the CFAA.[17] 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 paper 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 II explores the rise of the use of the CFAA to sue or prosecute employees who misappropriate confidential information. Part III summarizes the debate over the broad and narrow interpretations that have been ongoing in the federal courts over the past twelve years. Part IV focuses on the development of the *Nosal* case in the Ninth Circuit to expose how both the narrow and broad interpretations of "without authorization" and "exceeds authorized access" are applied to the same set of facts. Part V identifies the notable circuit split that the Ninth Circuit's interpretation creates with the First, Fifth, Seventh and Eleventh circuit courts of appeal. Part VI defends the Ninth Circuit's reasoning. The authors 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 by these terms.

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

The circuit split over the interpretation of terms in the CFAA is rooted in different views of the Act's purpose. Courts that urge adoption of a narrow view of the Act emphasize that its primary purpose is to punish hacking.[18] Courts taking a broader view, however, emphasize that the statute has been amended many times with the goal of punishing an increasing variety of activity related to computer misuse.[19]

The CFAA seeks to punish those who access computers "without authority" or who "exceed authorized access." Courts that interpret this language to apply primarily to hackers view the term "without authority" as applying to outsiders, those who hack into a computer system, with no authority whatsoever to access the computer or computer system; while the term "exceeding authorized access" would apply to insiders who have access to some programs or information but who go beyond those limits.[20] It is clear that an employee who goes beyond the limits based on a breach of code-based security has exceeded authorized access.[21] Such a transgression may also be identity theft.[22] Other crimes that damage computers or computer systems are also prohibited by the CFAA, such as distributing worms and denial-of-access attacks. [23]

---

[17] *Nosal IV*, 2012 U.S. App. LEXIS 7151 at *5-27.

[18] *See, e.g. id.* at *9; 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, at 495-96.

[19] *See supra* note 15 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).

[20] For a discussion of hackers and insiders who exceed authorized access, see Part VI.

[21] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes* , 78 N.Y.U. L. REV. 1596, 1643(2003) (recommending use breach of code-based access as trigger for "exceeding authorized access") [hereinafter Kerr, *Cybercrime's Scope*].

[22] *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) (discussing identity theft), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf [hereinafter DOJ Prosecution Manual]

[23] Kerr, *Cybercrime's Scope, supra* note 21, at 1603-04 (discussing these damaging acts); *see* DOJ Prosecution Manual, *supra* note 22, at 35 (noting virus or worm can use up all available bandwidth on employer's computer

The language of the CFAA, however, is susceptible to interpretations that encompass other types of computer misuse. Some courts have held that an employee who breaches a confidentiality agreement or acts with interests adverse to his employer has acted without authorization or has exceeded authorized access within the meaning of the statute. [24] A variety of theories have justified such interpretations. For example, some courts have used an agency theory, arguing that an employee has authorized access only as an agent to the employer.[25] Under this theory, the employee is "without authorization" once his interests diverge from those of his employer.[26]

Whether the statute is read narrowly to focus on violations such as hacking, or broadly to encompass an employee's misappropriation of confidential information, centers on the interpretation of the phrases "without authorization" and "exceeds authorized access." Section 1030(c) of the CFAA lists seven types of conduct punishable by fines or imprisonment.[27] Those usually invoked in cases involving an employee's misappropriation of confidential information are sections 1030(a)(2)(C), 1030(a)(4) and1030 (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 someone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."[28]

---

network thus denying employees access and delete files, crash computer, install malicious software, and in general do things to impair the computer's security; denial of service attacks flood victim's computer with useless information and prevents legitimate users from accessing it).

[24] *See* 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).

[25] *See* 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 he engaged in misconduct, destroying files that were employer property and breached duty of loyalty).

[26] *Id.* 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)).

[27] The seven provisions of the CFAA are summarized as:

> 1. Trespassing in a government computer, 18 U.S.C. 1030(a)(3) (Hacking);
> 2. trespassing resulting in exposure to certain governmental, credit, or computer-housed information,
> 18 U.S.C. (a)(2);
> 3. damaging a protected computer government computer, 18 U.S.C. (a)(5);
> 4. committing fraud an integral part of which involves unauthorized access to a protected computer;
> 5. threatening to damage a protected computer, 18 U.S.C. 1030(a)(7);
> 6. trafficking in passwords for a protected computer, 18 U.S.C. 1030(a)(6);
> 7. accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1)
> Attempt and conspiracy to commit these crimes are prohibited by section 1030(b).

See Charles Doyle, CSR Report for Congress, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, (Dec. 27, 2010) [hereinafter CSR Report].

[28] 18 U.S.C. § 1030 (a)(5)(c).

While it is clear that the CFAA is primarily a criminal statute, civil cases became common after a 1994 amendment provided a civil remedy to those harmed by the listed crimes.[29] Amendments in 1996 and 2008 further spurred civil litigation by broadening the definition of "protected computer." The statute originally protected "federal interest computers" but now the definition is so broad as to include any computer connected to the Internet.[30] These changes opened the door to allow suits by private employers against employees who misuse computers in a variety of ways.[31]

The CFAA might appear to be a reasonable vehicle for seeking remedies against disloyal employees. But the interpretations of the critical terms "without authorization" and "exceeds authorized access" that evolved in civil cases would set precedent for cases in the criminal context, with the potential to criminalize behavior far beyond that intended. Professor Orin Kerr, who has followed the development and changes in the statute closely, expressed concern that interpretations of critical terms in civil cases against employees would eventually have grave repercussions in the criminal context.[32] Kerr predicted that such broad interpretations would ultimately give prosecutors too much discretion in determining when an employee may be charged under the CFAA.[33]

The following section traces the development of the broad reading of the terms "without authorization" and "exceeds authorized access." The leading cases illustrate the various theories that support this interpretation. The section then illustrates how the theories that developed in civil cases were used in criminal cases.

III. DEVELOPMENT OF THE BROAD AND NARROW INTERPRETATIONS

A. Civil Cases – 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).[34] 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

---

[29] Subsection 1030 (g) states 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." 18 U.S.C. §1030(g). For a detailed description of the expansion of the CFAA see Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, at 1563-71 (2010). [hereinafter *Vagueness Challenges*].

[30] The definition is provided at 18 U.S.C. §1030(e)(2). The definition includes a computer "which is used in interstate commerce or communication." A further amendment in 2008 changed the definition to include computers "used in or affecting interstate or foreign commerce or communication." The addition of the phrase "or affecting" signals that Congress intended the term to be able to regulate to the full extent of its Commerce Clause power. *See* Kerr, *Vagueness Challenges*, *supra* note 29, at 1570.

[31] *See supra* note 15.

[32] *See* Kerr, *Cybercrime's Scope*, *supra* note 21, at 1641.

[33] See Kerr, *Vagueness Challenges*, *supra* note 29, at 1576-77 (noting CFAA "breathtakingly broad" and 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").

[34] 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).

the statute had expanded.[35] 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."[36]

One of the first cases to address the scope of the CFAA in the civil context was heard by the Court of Appeals for the First Circuit in 2001.[37] 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. 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.[38] 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 . . . ."[39]

The court focused on the confidentiality agreement that EF employees had 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. With little analysis, the court concluded that an employee exceeds authorized access when he breaches a broad confidentiality agreement.[40] 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."[41]

The Court of Appeals for the Seventh Circuit used the law of agency to interpret the extent of an employee's authorization. In *International Airport Centers v. Citrin*, the court found that an employee is "without authorization" once he violates a duty of loyalty to his employer.[42] 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.[43] 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.[44] The employee allegedly

---

[35] P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504 (3rd Cir. 2005)(citing Pacific Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003).
[36] *Id.*
[37] EF Cultural Travel BC v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).
[38] 18 U.S.C. §1030(a)(4).
[39] EF Cultural Travel BC v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001).
[40] *Id.* at 581.
[41] *Id.* at 583.
[42] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).
[43] *Id.*
[44] *Id.*

violated section 1030 (a)(5)(A)(1) which prohibits transmitting a program that "intentionally causes damage *without authorization* to a computer."[45] 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.[46]

The Seventh Circuit raised the issue of differentiating between the terms "without authorization" and "exceeds authorized access," a difference which the court characterized as "paper thin . . . but not quite invisible."[47] 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 *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.[48] 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.[49] 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 *Citrin* was first articulated in 2000 in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*.[50] In *Shurgard*, the court cited the Restatement (Second) of Agency in interpreting the meaning of "authorization."[51] Section 112 states: "Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[52] 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.[53] In defending this position, one court noted that this view appropriately focuses on initial access, not on subsequent misuse of the information.[54] The appropriateness of initial access under *Citrin*, however, necessarily hinges on the employee's intent at the time of access.[55]

B. Criminal Cases using the Broad Interpretation

---

[45] *Id.* (citing 18 U.S.C. §1030(a)(5)(A)(1)(emphasis added)).
[46] *Id.* at 420.
[47] *Id.* at 420 (citations omitted).
[48] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).
[49] *Id.* at 420-21.
[50] 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).
[51] *Id.*
[52] Restatement (Second) of Agency § 112 (1958).
[53] *See, e.g.*, NCMIC Finance Corp. v. Artino, 638 F. Supp. 2d 1042, 1059 (S.D. Iowa 2009); Guest-Tek Interactive Entertainment, Inc. v. Pullen, 665 F. Supp. 2d 42, 45-46 (D. Mass. 2009) (following broad interpretation of First Circuit in *EF Cultural Travel*, 274 F.3d 577, 582-84). *See generally*, Katherine Mesenbring Field, Note: *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 823-829 (2009) (discussing agency and contract-based interpretations).
[54] *See, e.g.*, NCMIC, 638 F. Supp. 2d at 1059 ("the broad view does not focus on an employee's later misuse of information but rather focuses on an employee's initial *access* of the employer's computer with the intent to either obtain information or defraud the employer . . . .").
[55] *See Citrin*, 440 F.3d at 42-21.

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. [56] Kerr worried that such interpretations would be applied to criminal cases, thereby "threaten[ing] a dramatic and potentially unconstitutional expansion of criminal liability in cyberspace."[57] 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.[58] 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.[59] Professor Kerr's concerns proved not to be unfounded. 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.[60] In *United States v. John*, an employee of Citigroup accessed confidential customer information and used that information to commit fraud.[61] 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.[62] 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.[63] 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.[64]

The court's decision in *John* is noteworthy for its expansive interpretation of the CFAA, but also because it reflects some discomfort with how decisions that interpret the statute broadly in the civil context might impact criminal cases. Noting that the First Circuit had found that an employee exceeds authorized access when he violates a broad confidentiality agreement, the Fifth Circuit agreed that the purpose for which access is authorized may determine whether an

---

[56] Kerr, *Cybercrime's Scope*, *supra* note 21, 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) . 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 use was implied because he knew that the worm would so invade the computers. 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.

[57] *See* Kerr, *Cybercrime's Scope*, *supra* note 21, at 1599.

[58] *See* EF Cultural Travel BC v. Explorica, Inc., 274 F.3d at 583; Field, *supra* note 53 at 820.

[59] *See* Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMPL. RTS. EMPLOY. POL'Y J. 11, 19 & 27 (2008) (noting "widespread endorsement" of *Shurgard* and that "Shurgard's approach is likely to stand.").

[60] United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).

[61] *Id.*

[62] *Id.* at 271.

[63] *Id.* at 272.

[64] *Id.* at 273.

employee has exceeded authorized access.[65] But the Fifth Circuit also stated that it "did not necessarily agree that violating a confidentiality agreement . . . would give rise to criminal culpability."[66] Such discomfort raises questions about the predictability of the broad interpretation.

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.[67] 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.[68] 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.[69]

In finding that Rodriguez had exceeded his authority under the CFAA, the Eleventh Circuit emphasized that Rodriguez had violated the employer's policy. [70] The Court was unpersuaded 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.[71] The Court concluded that the statute is clear that merely accessing the information by exceeding authorized access is criminal.[72] The Eleventh Circuit was not persuaded by 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 of the information is irrelevant if he obtained [it] without authorization or as a result of exceeding authorized access."[73]

---

[65] *Id.* at 272.
[66] *Id.*
[67] United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).
[68] *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.
[69] *Id.* at 1260.
[70] *Id.* at 1263.
[71] *Id.*
[72] *Id.*
[73] *Id.* at 1263. In *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. *Id.* at 1120. The appeal did not address whether or not 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. *Id.* at 1123-24.

The decisions by the Fifth and Eleventh Circuits indicate the breadth that the CFAA may have in the criminal context. In fact, because both of these cases involve issues of public trust such as data security, personal information and financial information, the decisions appear to conform to the original goals of the CFAA – which sought to protect such sensitive information.[74] The problem, however, lies not in the result, but in the process. In both *John* and *Rodriguez*, the employees were authorized to access the information in question. The courts, however, bypassed the inquiry into access to focus on the use of the material in John's case and the knowing violation of an employment policy in Rodriguez's case.

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.[75] 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.[76]

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 *LVRC Holdings v. Brekka*,[77] a decision which set forth the reasoning the court ultimately employed in its en banc decision in *United States v. Nosal*, with both the plain language approach and the rule of lenity figuring prominently in the court's reasoning. In *Brekka*, the court emphasized that it is the employer's action not the employee's state of mind that determines whether or not the employee had authorized access to the computer.[78]

---

[74] In Testimony before the United States House of Representatives, Professor Orin Kerr endorsed an amendment to a pending bill, S.1151 that would limit the scope of the CFAA. The proposed amendment would define "exceeds authorized access" as follows:

> Section 1030(e)(6) of title 18, United States Code, is amended by striking "alter;" and inserting "alter, but 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;"

Testimony of Orin S. Kerr, *Cyber Security: Protecting America's New Frontier: Hearing Before the Judiciary Subcomm. on the Crime, Terrorism, and Homeland Security* (Nov. 15, 2011), available at judiciary.house.gov/hearings/pdf/Kerr%2011152011. Kerr points out that this amendment would create an exception that would allow the government to prosecute for violations of computer use policies used by government employees, thus allowing for prosecution of government officials like Rodriguez. *Id.*

[75] *See, e.g.*, US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1192 (D. Kan. 2009); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (U.S. Dist. Ariz. 2008); Diamond Power Int'l v. Davidson, 540 F. Supp.2d 1322, 1342 (U.S. Dist. N.D. Ga. 2007); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 U.S. Dist. LEXIS 53108, at *15 (U.S. Dist. M.D. FL. Aug. 1, 2006).

[76] *See id.*

[77] 581 F.3d 1127 (9th Cir. 2009).

[78] *Id.* at 1135.

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 he left his place of employment, he emailed several documents to his personal email accounts. [79] LVRC alleged that Brekka violated sections 1030(a)(2) and (4) of the CFAA. The court considered whether or not Brekka had acted "without authorization" or "exceeded authorized access" under the CFAA in emailing the documents to his personal computer. [80] 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.[81] In interpreting these terms, the court sought a "sensible interpretation" that gave meaningful effect to both terms.[82] Because the statute does not define "without authorization," the court looked to its plain meaning, finding that "authorization" turns on whether or not an employer has granted the employee permission to use the company's computer.[83] Thus, the court found that "without authorization" means that an individual had "no rights, limited or otherwise, to access the computer in question."[84] The court cited hackers and employees whose access has been rescinded or terminated as those "without authorization."[85]

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.[86] 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.[87] The court rejected the Seventh Circuit's interpretation of "without authorization," finding that the plain language of the CFAA does not support an argument that an employee is "without authorization" if he uses the computer "contrary to his employer's interest"[88] or breaches "a state law duty of loyalty to an employer."[89]

---

[79] *Id.* at 1129-30.

[80] 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). 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).

[81] 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. *Id.* at 1136-37.

[82] *Id.* at 1133.

[83] *Id.*

[84] *Id.*

[85] *Brekka*, 581 F.3d at 1135.

[86] *Id.*

[87] *Id.* at 1128.

[88] *Id.*

[89] *Id.* at 1135.

The court noted that its interpretation of terms in the CFAA had to be consistent whether a case was brought in either a civil or criminal context. [90] 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 its narrow interpretation of the terms "without authorization" and "exceeds authorized access."[91] The court found that a broad interpretation of these phrases would not adequately notify employees about what type of behavior is criminal.[92]

Although the Ninth Circuit's decision in *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 *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,"[93] but suggested nonetheless that its decision could be read consistently with the Ninth Circuit's decision in *Brekka*. [94] The Fifth Circuit's decision notes that in *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. [95] In *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.[96] The Fifth Circuit suggested that *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."[97]

The Eleventh Circuit also sought to distinguish its decision in *Rodriguez* from *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 form emailing company documents to personal email accounts, [98] he was in a different position than Rodriguez who knew he was not authorized to obtain personal information for nonbusiness reasons.[99]

The Court of Appeals for the Sixth Circuit, however, gave some weight to the narrow view articulated in *Brekka.* In *Pulte Homes v. Laborers' International Union of North America*,[100] the court interpreted the term "without authorization" narrowly. After an employee was fired from

---

[90] *Id*. at 1134.
[91] *Id.*
[92] *Id.* at 1135.
[93] *John*, 597 F.3d at 272.
[94] *Id.* at 273.
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Rodriguez*, 628 F.3d at 1263 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009)).
[99] *Id.*
[100] 648 F.3d 295 (6th Cir. 2011). A 2012 decision in the United States Court for the Eastern District of Michigan states that "Pulte suggests the Sixth Circuit would adopt a narrow interpretation of the CFAA when the issue presents itself in the context of an employment dispute . . . ." Ajuba Int'l, LLC v. Saharia, No. 11-12936, 2012 U.S. Dist. LEXIS 66991, at *31 (E.D. Mich. May 14, 2012). In *Ajuba*, the court adopted the narrow reading of the CFAA. *Id*. at *32.

Pulte Homes, the labor union initiated a phone and email blitz that disrupted Pulte's system.[101] 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 not "unauthorized."[102] 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.[103] The court concluded that "without authorization" means "no permission to access whatsoever."[104]

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.[105] The facts in *Nosal* were similar to those in *Brekka*, *EF Cultural*, and *Citrin*, involving an employee who stole a former employer's information.[106] But the case was raised in the criminal context.[107] 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 adopt the broad or narrow view.[108] The summary of the Ninth Circuit's en banc decision reveals that the court answered any lingering questions about the reach of the *Brekka* decision and clearly defines the parameters of the terms "without authorization" and "exceeds authorized access."[109]

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

The *Nosal* case, like *Brekka*, involved employees who stole confidential information from an employer to set up a competing business. *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.[110] 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.

---

[101] *Pulte*, 648 F.3d at 299.
[102] *Id.* at 304.
[103] *Id.* at 303-04.
[104] *Id.* (citing Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. Aug. 1, 2006).
[105] United States v. Nosal, No. 10-10038, 2012 U.S. App. LEXIS 7151 at *7 (9th Cir. April 10, 2012) (*Nosal IV*).
[106] *Id.* at *3.
[107] *Id.*
[108] *Id.* at *4; *see infra* Part IV discussing the *Nosal* decisions.
[109] *Id.* at **9-24.
[110] United States v. Nosal, No. C 08-0237 MHP, 2010 U.S. Dist. LEXIS 24359, at *3 (N.D. Cal. Jan. 6, 2010) [hereinafter *Nosal II*].

Nosal was indicted for trade secret theft, mail fraud, and violations of the CFAA.[111] The CFAA count was based on section 1030(a)(4) which punishes someone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access . . . ."[112] The government maintained that Nosal had violated this section of the CFAA by aiding and abetting the Korn/Ferry employees in exceeding their authorized access with intent to defraud.[113] 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.[114]

The United States District Court for the Northern District of California originally adopted the broad interpretation of "without authorization" and "exceeds authorized access."[115] The court found that Nosal violated the CFAA because he accessed the employer's computer and confidential information with "nefarious intent," meaning interests contrary to those of his employer or in violation of his contractual agreements.[116]

After the Court of Appeals for the Ninth Circuit decided *Brekka*, the district court reconsidered its decision in *Nosal*.[117] Building on the distinction the court made in *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."[118] 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.'"[119] The court concluded that the statute cannot reasonably be read to allow "alter" to mean "misappropriate."[120] Thus, the court applied the reasoning in *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.[121]

In 2011, a three-judge panel of the United States Court of Appeals for the Ninth Circuit reversed the district court's decision.[122] 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."[123] 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 *so* to obtain or alter."[124] The

---

[111] United States v. Nosal, No. CR 08-00237 MHP, 2009 U.S. Dist. LEXIS 31423 (N.D. Cal. Apr. 13, 2009) [hereinafter *Nosal I*].
[112] 18 U.S.C. § 1030(a)(4) (2012).
[113] *Nosal II*, 2010 U.S. Dist. LEXIS 24359, at *3.
[114] *Nosal II*, 2010 U.S. Dist. LEXIS 24359, at **18-20.
[115] *Id.*
[116] *Id.* at *10 (citing *Nosal I*, 2009 U.S. Dist. LEXIS 31423, at **6-7).
[117] *Nosal II*, 2010 U.S. Dist. LEXIS 24359, at *2.
[118] *Id.* at *16.
[119] *Id.* at *20 (citing 18 U.S.C. §130(e)(6)).
[120] *Nosal II*, 2010 U.S. Dist. LEXIS 24359, at **20-21.
[121] *Id.* at *22.
[122] United States v. Nosal, 642 F.3d 781 (9th Cir. 2011) [hereinafter *Nosal III*].
[123] *Id.* at 782.
[124] 18 U.S.C. § 1030(e)(6) (2012).

court used a dictionary definition of "so" to mean "in a manner or way that is indicated or suggested."[125] Thus, the court concluded that an employee who accesses information in a manner to which he is not entitled, has exceeded authorized access. [126]

The court distinguished the instant case from *Brekka* because of factual differences. In *Brekka*, the court noted, the employee 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. [127] By contrast, Nosal and the Korn/Ferry employees were subject to a clear and conspicuous computer policy with specific restrictions.[128]

Furthermore, the Ninth Circuit found that the rule of lenity which supported its narrow interpretation of terms in *Brekka* did not apply to the circumstances in *Nosal*.[129] 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."[130] The situation in *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.[131]

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 its previous decision. The court held 9-2, that the CFAA does not extend to violations of an employer's use restrictions, reasoning that Congress must speak more clearly if it wants to incorporate misappropriation liability into the CFAA.[132] 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.[133] Impermissible access, the court reasoned, must be determined by considering whether an employee has "circumvent[ed] technological barriers."[134]

In reaching this conclusion, the court paid close attention to principles of statutory construction, but its overriding concern was for 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 use in violation of an employer's computer use policy - such as sending personal email, checking sports scores, or playing Sudoku.[135] The court noted that employees are seldom disciplined for violating computer use policies, and therefore cautioned that a broad interpretation of the CFAA

---

[125] *Nosal III*, 642 F.3d at 785.
[126] *Id.* at 785-86.
[127] *Id.* at 787.
[128] *Id.*
[129] *Id.* at 786-87.
[130] *Id.* at 787-88.
[131] *Id.* at 786.
[132] United States v. Nosal, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *25 (9th Cir. Apr. 12, 2012) [hereinafter *Nosal IV*].
[133] *Id.* at *26.
[134] *Id.*
[135] *Id.* at *17.

would allow employers to threaten to report minor violations by "troublesome employees" to the FBI.[136] 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."[137]

The court cited several problems associated with interpreting the CFAA to include 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.[138] Second, the court characterized computer use policies and terms of service as broad, vague, opaque, subject to change, and frequently unknown.[139] Such characteristics, the court noted, raise serious questions regarding adequate notice to employees about what constitutes criminal behavior. [140] For example, the court asked, what does "nonbusiness" use mean? [141] 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.[142] These problems, inherent in a broad interpretation 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."[143]

The court cited a few examples of the far-reaching effects a broad reading of the CFAA could have. In *United States v. Drew*, a woman was prosecuted under the CFAA for creating a false profile on MySpace.com.[144] In lying about the information in the profile, the woman violated MySpace's terms of service, thereby subjecting her to a claim that she exceeded authorized access under the CFAA.[145] 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.[146] Although the CFAA claims were dismissed in both of these suits, the Ninth Circuit illustrated 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."[147]

While the thrust of the Ninth Circuit's decision is its concern that a broad reading of the CFAA could turn "minor dalliances" into "federal crimes,"[148] the decision includes careful analysis of the statutory language and legislative history. The court rejected the government's attempt to

---

[136] *Id.* at **14-15.
[137] *Id.* at *18.
[138] *Id.* at *16.
[139] *Id.* at **16-21.
[140] *Id.* at *21.
[141] *Id.* at *16-17.
[142] *Id.* at **21-22.
[143] *Id.* at *17.
[144] *Id.* at *22 (citing United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)).
[145] *Nosal IV*, 2012 U.S. App. LEXIS 7151, at *22.
[146] *Id.* at *15 n.6 (citing Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742038 (M.D. Fla. May 6, 2011)).
[147] *Nosal IV*, 2012 U.S. App. LEXIS 7151, at *21.
[148] *Id.* at *14.

read the definition of "exceeds authorized access" to include use restrictions.[149] 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".[150] 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."[151] The court stated that Congress would likely use much more straightforward language if it intended to criminalize violations of computer use restrictions.[152] 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.'"[153]

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.[154] 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 that section punishes those who exceed authorized access "knowingly and with intent to defraud."[155] 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.[156] 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.[157] 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.[158]

V. CIRCUIT SPLIT

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."[159] The First, Fifth, Seventh, and Eleventh Circuits have all analyzed the term "exceeds authorized access" under the CFAA and have found that an employee "exceeds authorized access" in the following situations: the employee violates a broad confidentiality agreement;[160] the employee violates a duty of loyalty to his employer;[161] the employee accesses

---

[149] *Id.* at **6-9.
[150] *Id.*
[151] *Id.* at *7.
[152] *Id.*
[153] *Id.* at *7 n.3 (citing 18 U.S.C. § 1832 (2012)).
[154] *Nosal IV*, 2012 U.S. App. LEXIS 7151, at *13.
[155] *Id.* at *12.
[156] *Id.* at *13 (citing Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007) ("identical words and phrases within the same statute should normally be given the same meaning")).
[157] *Nosal IV*, 2012 U.S. App. LEXIS 7151, at *14.
[158] *Id.*
[159] *Id.* at *30-31(Silverman, J., dissenting).
[160] EF Cultural Travel BC v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001).
[161] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

information with a criminal purpose;[162] or the employee knowingly violates an employment policy.[163] 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.[164]

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 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.[165] The majority, however, makes it clear that the Ninth Circuit interprets the terms "without authorization" and "exceeds authorized access" in a more literal manner and that the *Brekka* decision does not allow for interpretations that would target "misuse or misappropriation" of information.[166]

While there are no circuit court of appeal decisions that expressly agree with the Ninth Circuit's interpretation of the CFAA in *Nosal IV*, the Sixth Circuit notably adopted a similar view regarding authorization to access in *Pulte Homes*,[167] and recent decisions suggest that the narrow view is gaining momentum in the federal district courts.[168] 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.[169] 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."[170] 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.[171]

Several district courts within the Second Circuit have also adopted the narrow approach.[172] In a recent criminal case, *United States v. Aleynikov*, the United States District Court for the Southern

---

[162] United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).
[163] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).
[164] *Nosal IV*, 2012 U.S. App. LEXIS 7151, at *5.
[165] *Id.* at *29 (Silverman, J., dissenting).
[166] *Id.* at *24 (citing Shamrock Foods Co. v. Gast, 535 F. Supp.2d 962, 965 (D. Ariz. 2008)).
[167] *See* Pulte Homes, Inc. v. Laborers' Int'l Union of North America, 648 F.3d 295, 304 (6th Cir. 2011). The Sixth Circuit read the term "without authorization" narrowly when finding that a union had authorized access to the plaintiff's phone and email, both of which were open to the public. *See supra* at note 100 regarding *Pulte.*
[168] *See, e.g.*, 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 Services, Inc. v. Barney, 698 F. Supp.2d 1309, 1315-16 (M.D. Fla. 2010) (adopting narrow view and rejecting *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*).
[169] No. 11-2673 (DSD/AJB), 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.
[170] *Id.* at **5-6 (citing two cases in 2011 in the District of Minnesota that followed the narrow view and one 2006 case that favored a broader approach).
[171] *Id.* at *11.
[172] *See* United States v. Aleynikov, 737 F. Supp.2d 173, 191-94 (S.D.N.Y. Sept. 3, 2010*);* Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp.2d 378 (S.D.N.Y. July 14, 2010); Orbit One Commc'ns, Inc. v. Numerex Corp.,

District of New York clearly articulated its preference for the approach taken by the Ninth Circuit in *Brekka*, and ultimately, in *Nosal IV*.[173] Notably, the court stated in *Aleynikov*, "[w]hat use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place."[174] 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.[175]

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 Ninth Circuit makes it clear that the CFAA is not a statute that should be used to punish employees who use their access to misuse information.[176] 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. [177] According to the Ninth Circuit, these courts 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.'"[178]

While the circuits clearly disagree on how to interpret authorization under the CFAA, the cases reveal some interesting differences. In *Nosal* and in *Aleynikov*, the courts rejected the CFAA as a means of criminalizing an employee's misappropriation of information, refusing to punish employees who harmed their employer. In *United States v. John* and *United States v. Rodriguez*, however, the courts found that employees could be liable for violating an employer's policy that harmed innocent third parties. In *John*, innocent people were victims of fraud; in *Rodriguez*, innocent people suffered an invasion of privacy. In both *John* and *Rodriquez*, the courts were concerned with the fact that sensitive, personal information was involved. Furthermore, the cases involved the types of institutions that were the initial focus of the CFAA – a financial institution in *John*, a government agency in *Rodriguez*. While interpretations of the authorization terms must be consistent throughout the statute, it is worth recognizing that in *John* and *Rodriguez* the courts were focusing on third party victims, not employers.[179]

---

692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Jet One Group, Inc. v. Halcyon Jet Holdings, Inc., No. 08 Civ. 3980 (JS), 2009 U.S. Dist. LEXIS 72579 (E.D.N.Y. Aug. 14, 2009).

[173] *Aleynikov*, 737 F. Supp.2d at 191-94.

[174] *Id.* at 192.

[175] *See* United States v. Aleynikov, No. 11-1126, 2012 U.S. App. LEXIS 7439 (2nd Cir. Apr. 11, 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 *2. 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.*

[176] *Nosal IV*, 2012 U.S. App. LEXIS 7151, at *3.

[177] *Id.* at *23 (citing United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2020); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006)).

[178] *Nosal IV*, 2012 U.S. App. LEXIS 7151, at *3.

[179] The position taken by the Fifth and Eleventh Circuits reflects the concern that Congress had in protecting private information. The legislative history of the CFAA demonstrates this concern. In revising the definition of "exceeds authorized access" the Senate Report considered whether "obtaining information" in Section 1030(a)(2) would require proof of "asportation of the data in question." See S. REP. No. 99-432, at 6-7 (1986), reprinted in 1986 U.S.C.A.A.N. 2479, 2486. The legislative history stated that "[b]ecause the premise of this subsection is privacy

Closely connected to the circuit split over defining authorization terms is the growing disagreement over how to interpret the "damage" and "loss" provisions of the CFAA. Like the dispute over authorization terms, much of the debate focuses on whether or not the CFAA contemplates suits that allege misappropriation of confidential information.[180] Several courts have stated that misappropriation of confidential information alone does not satisfy the damage and loss provisions.[181] Courts that follow the broad reading of the statute conclude that accessing and disclosing trade secrets can constitute an impairment to the integrity of data or information.[182]

The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[183] "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."[184] The language in these sections indicates the type of harm caused by hacking or altering information on a system, not loss associated with disloyal employment practices or theft of trade secrets.[185] Some courts have been reluctant to read the term "damage" too expansively, stating that "damage" under the CFAA refers to "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.'"[186] Thus, 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

---

protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection." *Id.* Thus, this legislative history indicates that the fact that an unauthorized accesser *viewed* the information as opposed to removing or copying it, could amount to a violation because the "premise of [the] subsection is privacy protection." *Id.* at 6. Nevertheless, this emphasis on privacy protection does not obviate the need to prove that access was exceeded to view the information.

[180] *See* Consulting Professional Resources, Inc. v. Concise Technologies LLC, No. 09-1201, 2010 WL 1337723 (W.D. Pa. March 9, 2010) (nothing that the debate over "what constitutes 'damages' under the CFAA falls victim to similar debate" as conflict over interpreting authorization terms).

[181] *See id.* at *8 ("compromise or decrease in the competitive value of . . . confidential information does not satisfy the damage requirement . . . .); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 U.S. Dist. LEXIS 53108, at *26 (U.S. Dist. M.D. FL. Aug. 1, 2006) (holding that copying confidential information is not damage under the CFAA). *See also* Black & Decker 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), even when no data, program, or system is damaged or destroyed").

[182] *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, No. 04 C 1606, 2004 WL 1197395, at *4 (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 suggests 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.*

[183] 18 U.S.C. § 1030(e)(8).

[184] 18 U.S.C. § 1030(e)(11).

[185] *See generally* Warner, *supra* note 59, 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).

[186] *See, e.g.*, Triteq Lock & Security, LLC v. Innovative Secured Solutions, LLC, No. 10 CV 1304, 2012 U.S. Dist. LEXIS 14147, at * (Feb. 1, 2012).

meaning of the statute.[187] Some courts have also limited the meaning of "loss" to costs associated with interruption of service and investigation or response to computer damage or intrusion.[188] Interpretations of the terms "damage" and "loss" arise from a variety of concerns, but conclusions as to the breadth of the terms are closely tied to the debate over the scope of authorization terms.

VI. DEFENDING THE NARROW INTERPRETATION OF "EXCEEDING AUTHORIZED ACCESS"

The *Brekka* and *Nosal* decisions gave the Ninth Circuit ample opportunity to consider the CFAA's language, intent, and impact. Through comprehensive consideration and reconsideration of terms in the CFAA, the Ninth Circuit has weighed a variety of well-reasoned arguments for broad, narrow, and nuanced readings of the terms "without authorization" and "exceeds authorized access." Thus, although the dissent accused Chief Judge Kozinksi, who authored the en banc decision, of "conjur[ing] up far-fetched hypotheticals," and "knocking down straw men,"[189] the decision is well-informed by the court's extensive consideration of these issues and the potential impact of its interpretations.

The following section defends the Ninth Circuit's narrow reading of the CFAA. First, it considers the overall objectives of the statute which emphasize hacking rather than misappropriation of confidential information. It 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. Thus, a review of the legislative history, which is ambiguous, is largely superfluous. The rule of lenity and due process considerations further support the narrow view. This section then considers the impact that the CFAA has on misappropriation laws, concluding that a narrow interpretation of the statute prevents further unanticipated consequences.

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

[187] Pulte Homes, Inc. v. Laborers' Int'l Union of North America, 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 access to the system. *Id.* at 304. In *Ajuba International, LLC. v. Saharia*, No. 11-12936, 2012 U.S. Dist. LEXIS 66991, at *31 (E.D. Mich. May 14, 2010), a federal district court within the Sixth Circuit's jurisdiction recently 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 court's reliance upon the Ninth Circuit's decision in *Brekka*.

[188] *See* Bashaw v. Johnson, No. 11-2693-JWL, 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. Marketcliq, Inc., 6:11-cv-1011-Orl-36DAB, 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").

[189] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *27-28 (9th Cir. April 10, 2012) (Silverman, J., dissenting).

Courts adopting the narrow view have emphasized that the CFAA sought to criminalize the type of computer abuse commonly referred to as external hacking.[190] Examples of external hacking portrayed in the media typically glamorize hacker conduct, often implying that hackers are geniuses with the daring of James Bond.[191] The 1986 Senate Report stated that "programs should be implemented that deflate the myth that computer crimes are glamorous, harmless pranks."[192] The myth still persists, however, as can be seen by the popularity of films such as "The Girl with the Dragon Tattoo."[193] 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.[194]

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.[195] 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 many computers to shut down.[196] The media conveyed a larger-than-life depiction of the monetary impact of Morris's hacking.[197] In 1988, the impact of the Morris worm was primarily on large institutions because home computing was in its infancy.[198] The Court of Appeals for the Second Circuit found that Morris had sufficient intent to violate section 1030 (a)(5)(A) 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."[199] Robert's punishment was light, and MIT seemingly held no lasting animosity towards him because he later became a tenured member of the faculty there.[200]

---

[190] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009) (quoting H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984). *See* Urban *supra* note 9 at 1369 (noting hackers and outsiders as original focus of legislation).

[191] *See* Michael P. Dierks, *Symposium: Electronic Communications and Legal Change: Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 315 & n.22 (2003)(citing KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER (1991) for proposition that most hackers are more like Pee Wee Herman than James Bond or Einstein).

[192] S. REP. No. 99-432, at 3 (1986).

[193] 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 2 at ¶4 (discussing portrayal of Matthew Broderick as whiz kid computer hacker in 1983 film War Games where Broderick's conduct led United States to brink of nuclear war with the Soviet Union).

[194]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.

[195] *See* Kerr, *Vagueness Challenges*, *supra* note 29, at 1563.

[196] *See* Hackers, Frontline, PBS, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html (last visited May 26, 2012). Morris unleashed the worm at MIT.

[197] *See* Dierks, *supra* note 188, 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 (1991) (convicting Morris of violating CFAA for intentionally unleashing a worm on the early Internet that caused numerous institutional systems to cease functioning).

[198] *See* GERALD R. FERRERA ET AL., CYBERLAW TEXT AND CASES 10 (3d ed. 2012) (noting first commercial use of Internet in 1988 with dial up available to consumers in 1989).

[199] *Morris*, 928 F.2d at 507, 511.

[200] *See* Robert Morris, *Pioneer in Computer Security, Dies at 78*, N.Y. TIMES, June 29, 2001, *available at* http://www.nytimes.com/2011/06/30/technology/30morris.html (discussing son Robert Morris who wrote the software program "worm" that resulted in his prosecution under the CFAA); *see also 5 Old School Hackers, Where*

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.[201] The same year, Gonzalez was indicted for theft of credit card information from Heartland Payment Systems, information he used to create counterfeit credit cards.[202] 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.[203] Hotz was also well-known for "jailbreaking" Apple's iPad and iPhone, so that the devices could be used with multiple wireless carriers.[204]

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 increase his bargaining power for a raise.[205] 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 focus on external and internal hacking.[206] 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."[207]

B. Rules of Statutory Construction Support a Narrow Reading

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. [208] In

---

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).

[201] *See* Desiree Baughman, *Internet Age: Five Memorable Cyber Crimes*, INSURANCE QUOTES (March 26, 2012), http://www.insurancequotes.org/2012/03/26/internet-age-five-memorable-cyber-crimes/ ; Declan McCullagh, *T.J. Maxx hacker sentenced to 20 years in prison*, CNET NEWS (March 25, 2010, 2:36 pm PDT), http://news.cnet.com/8301-13578_3-20001207-38.html .

[202] *See* Baughman, *supra* note 199.

[203] PARMY OLSON, WE ARE ANONYMOUS 226 (Little Brown 2012).

[204] *Id. See also* George Hotz Entry, WIKIPEDIA, http://en.wikipedia.org/wiki/George_Hotz (last visited May 27, 2012) (noting his notable hacks and that the Sony suit settled).

[205] *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).

[206] *See* Kerr, *Cybercrime's Scope*, *supra* note 21, 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).

[207] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *26 (9th Cir. April 10, 2012).

[208] *See, e.g., id.* (using plain language analysis, legislative history, and rule of lenity); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134-35 (9th Cir. 2009) (relying on plain language of the statute and rule of lenity); Black &

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 make some provisions superfluous or would create absurd results; interpreting provisions that apply to criminal and civil sanctions in the same manner; avoiding interpretations that create constitutional failings because of lack of notice as to the crime resulting in judicial determination that the provision 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.

1. Plain Meaning

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.[209] The "fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning."[210] The phrase "without authorization" is not defined in the CFAA.[211] 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"[212] or "entitled."[213] 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.[214] In evaluating the CFAA, some courts have seen no ambiguity in the phrase

---

Decker v. Smith, 568 F. Supp. 2d 929, 934-35 (W.D. Tenn. 2008) (same); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965-67 (D. Ariz. 2008) (using plain language analysis , legislative history, and rule of lenity).

[209] *See, e.g., Nosal IV*, (2012 U.S. App. LEXIS 7151, at **25 (holding that "the phrase 'exceeds authorized access' in the CFAA does not extend to use restrictions"); Orbit One Commc'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.").

[210] 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).

[211] *See* Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J. L.TECH. 233, 236 & n.21 (2010).

[212] *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.").

[213] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *5-6 (9th Cir. April 10, 2012).

[214] 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 207, at 247 -56 (2010) (discussing computer security model of CFAA interpretation including access control lists).

"without authorization" and refused to consider further extrinsic evidence to elucidate the language.[215]

"Exceeding authorized access" has proved to be the more frequently litigated term, even though the statute provides a definition.[216] 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."[217] 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.[218] The court in *Lockheed Martin* gives one 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).[219]

The narrow interpretation of authorization terms has the advantage of an objective assessment of whether or not the employee had permission to access the information in question. Broad interpretations of the authorization terms rely on an employee's subjective intent when he accesses confidential information.[220] There is nothing in the statute that links authorization to

---

[215] *See* Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 U.S. Dist. LEXIS 53108, at *15 (U.S. Dist. 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 53, 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").

[216] *See* DOJ IP Manual, *supra* note 10 at 12, 14 (noting most litigated issue about "exceeding authorized access" is whether exceeded by accessing for improper purpose).

[217] 18 U.S.C. § 1030(e)(6) (2012).

[218] *See, e.g., Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *24 (9th Cir. April 10, 2012) ("the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation'" (citing Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (internal quotation marks omitted); Black & Decker v. Smith, 568 F. Supp. 2d 929, 935 ("the plain meaning of 'exceeds authorized access' is 'to go beyond the access permitted'") (citing *Lockheed Martin*, 2006 U.S. Dist. LEXIS 53108, at *19). *See also* Field, *supra* note 53, at 821 (discussing vague authorization language in CFAA that courts have had difficulty applying to the "delicate and complex relationship that exists between employers and employees").

[219] Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *14 (M.D. Fla. Aug. 1, 2006).

[220] *See, e.g.*, NCMIC Finance Corp. v. Artino, 638 F. Supp. 2d 1042, 1059 (S.D. Iowa 2009)(adopting the broad view and explaining that "the broad view does not focus on an employee's later misuse of information but rather focuses on an employee's initial *access* of the employer's computer with the intent to either obtain information or defraud the employer . . . ."). *See also* United States v. Aleynikov, 737 F. Supp. 2d 173, 193 (S.D.N.Y. 2010) (criticizing the broad interpretation because it would "require an analysis of an individual's subjective intent in

intent.[221] One court noted that the *Citrin* analysis would suggest that an employee's authorization status could shift throughout his employment, depending on his state of mind at the time of access.[222] The court stated that "Congress could not have intended a person's criminal and civil liability to be so fluid, turning on whether a person's interests were adverse to the interests of an entity authorizing the person's access."[223] 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 would violate the principle of statutory construction that "identical words and phrases within the same statute should normally be given the same meaning."[224]

The narrow approach has the further advantage of giving a sensible construction to both "without authorization" and "exceeds authorized access."[225] 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*.[226] Courts have criticized the reasoning 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."[227] The Supreme Court noted in an environmental case 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."[228] 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."[229] In *Nosal IV*, the court pointed to some discussion of the definition of "exceeds authorized authority" that supports a narrow meaning.[230]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

---

accessing a computer system"); Ajuba Int'l, LLC v. Saharia, No. 11-12936, 2012 U.S. Dist. LEXIS 66991, at *33 (E.D. Mich. May 14, 2012) (agreeing with criticisms of the broad interpretation).

[221] *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.").

[222] *See* Lewis-Burke Associates, LLC v. Widder, 725 F. Supp. 2d 187, 193-94 (D.D.C. 2010).

[223] *Id.* at 194 (citations omitted).

[224] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *13 (9th Cir. April 10, 2012) (citing Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007).

[225] *See Brekka*, 581 F.3d at 1133.

[226] *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").

[227] US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009) (citing Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (U.S. Dist. Ariz. 2008)).

[228] Whitman v. American Trucking Assoc., 531 U.S. 457 (2001)(citations omitted).

[229] *See, e.g.*, Kerr, *Cybercrime's Scope, supra* note 21, at 1616 (noting difficulties regarding meanings of access and authorization legislatures never resolved).

[230] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *10 n.5 (citing S. REP. No. 99-432, at 21).

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 . . . ."[231]

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 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."[232] The legislative intent was clear that there was a preference for administrative rather than criminal sanctions in cases where such an individual exceeded access.[233]

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.[234] 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.[235]

Proponents of the broad interpretation of the CFAA can find favorable arguments in the legislative history as well. For example, courts cite amendments to the statute as support for Congress's intent to expand its 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.[236] These amendments, however, are more appropriately read to allow private employers to recover for damages related to computer misconduct involving hacking rather than misappropriation of confidential information.[237]

3. Void for Vagueness and the Rule of Lenity

Although the legislative history of the CFAA is ambiguous regarding the definition of authorization, the narrow interpretation 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

---

[231] S. REP. No. 99-432, at 21 (1986), reprinted in 1986 U.S.C.C.A.N. 2480-81 (citing Report on Computer Crime; Task Force on Computer Crime, Section of Criminal Justice, American Bar Association; June 1984).
[232] *Id.* at 7.
[233] *Id.*
[234] *Id.* at 3.
[235] *See id.*
[236] *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").
[237] See discussion *supra* at text accompanying notes 178-86.

the coverage of the first federal criminal statute.[238] The rule requires that any ambiguity in a criminal statute be resolved in favor of the defendant. The purpose of the rule is to ensure notice and legislative supremacy.[239] The notice theory prevents criminals from being caught off guard by interpretations of statutes that they could not reasonably have anticipated, while ensuring legislative supremacy provides a guarantee that courts will not exceed the legislative intent behind the statute.[240] A vague law may authorize and even encourage arbitrary and discriminatory enforcement."[241] To avoid such vagueness concerns, the doctrine requires that courts construe criminal laws narrowly to cure the vagueness.[242]

In the recent case of *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."[243] Thus, in the *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.[244]

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 *Nosal IV*, employees and consumers are usually unaware of what such cumbersome agreements prohibit.[245]

Both the rule of lenity and the void-for-vagueness doctrine call for a narrow interpretation of criminal conduct in the face of any 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. [246] Similarly, in *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

[238] United States v. Wiltberger, 18 U.S. (5 Wheat.) 76, 95, 105 (1820).
[239] *See* Zachary Price, *The Rule of Lenity as a Rule of Structure*, 74 FORDHAM L. REV. 885, 885 (2004).
[240] *Id*. at 886.
[241] *See* Chicago v. Morales, 527 U.S. 41, 52 (1999) (citing Kolender v. Lawson, 461 U.S. at 352, 358(1983)).
[242] *See* Kerr, *Vagueness Challenges*, *supra* note 29, at 1573 & n.91 (citing City of Chicago v. Morales, 527 U.S. at 41, 64, 92, 112).
[243] Skilling v. United States, 130 U.S. 2896, 2906, 2927-28 (2010) (citing Kolender v. Lawson, 461 U.S. at 352, 357 (1983)).
[244] *Id.* at 2896, 2906 (2010). Justice Ginsburg writing for the majority cautioned against extending 'honest services' beyond its core meaning for it "would encounter a vagueness shoal." *Id.* at 2907.
[245] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *18 (9th Cir. 2012).
[246] *See* Warren Thomas, *Lenity on Me*: LVRC Holdings LLC v. Brekka *Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act,* 27 GA. ST. U. L. REV. 379, 399-400 (2011) Thomas referred to Justice Scalia's statement that "the tie must go to the defendant" according to the rule of lenity. *Id.* at 407, n.197 (citing United States v. Santos, 553 U.S. 507, 514 (2008) (Scalia, J., plurality opinion)).

a state law duty of loyalty to an employer . . . . It would be improper to interpret a criminal statute in such an unexpected manner."[247]

The canon of avoiding absurd results is also important in defeating arguments for a broad interpretation.[248] In *Nosal IV*, the court anticipates that a broad reading of the CFAA could lead to absurd results.[249] The court provides an example of an employee who "spends six hours tending his Farmville stable on his work computer."[250] 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.[251]

C. A Narrow Interpretation Prevents Intrusion on Misappropriation Laws

In addition to strong arguments based on plain language analysis and canons of statutory construction, courts must be mindful that employees' disloyal behavior is prohibited by other federal and state laws. In *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.[252] The court also stated that contract and tort law have been the domain of misappropriation law. [253] Courts that have explored the limits of the CFAA in the employment context have merely 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.[254] A narrow reading of the CFAA would avoid such problems.[255]

Reading the CFAA narrowly is not a question of letting underhanded and dishonest employees go unpunished, but the statute should not be used to make it easier for employers or prosecutors to make their case. Plaintiffs and prosecutors have 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, the defendant may be charged with mail fraud and trade secret theft under the Electronic Espionage Act (EEA) as Nosal was.[256]

In several cases, employers have sought relief under the CFAA for claims that involve theft of trade secrets.[257] The fact that the EEA does not allow a private right of action for trade secret

---

[247] LVRC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009).
[248] *See* Booms, *supra* note 7 at 555; Kerr, *Vagueness Challenges*, *supra* note 29, 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).
[249] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151 (9th Cir. 2012), at * 26 (Chief Justice 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]).
[250] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151 (9th Cir. 2012), at *15, n.7.
[251] *Id.*
[252] *Id.* at *7-8 & n.3.
[253] *Id*. at *16.
[254] *See* Brenton, *supra* note 6, at 430-31.
[255] *See id.* at 454-55, 460-61.
[256] *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151 (9th Cir. 2012), at *3.
[257] *See, e.g.*, *Nosal IV*, No. 10-10038, 2012 U.S. App. LEXIS 7151, at *26 (9th Cir. 2012) (refusing to hold CFAA covers misappropriation of trade secrets).

theft makes it highly unlikely that Congress intended to provide such a remedy through the CFAA. A broad interpretation of the CFAA allows an employer to clear the authorization hurdle easily and succeed on his claim with much less effort than he would under the EEA or a state trade secret theft statute.[258] The employer can receive damages under the CFAA merely by proving that the information was on a computer, that the defendant obtained that information through unauthorized access or access exceeding existing authorization, and that he has suffered damage or loss.[259] 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.[260] Thus, one commentator states that "[s]ince the evidentiary elements of proof of a CFAA (a)(2)(C) 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."[261]

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." As presently written, however, the Ninth Circuit's view 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 employers. Rather, they seek to avoid the unintended consequences of a broad reading of the CFAA, most notably criminalizing innocuous behavior and disrupting trade secret law. 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 prosecution of misappropriation of confidential information to laws specifically tailored to that end.

---

[258] *See* Brenton, *supra* note 6, at 440.
[259] *Id.* at 438-89.
[260] *Id.* at 443-44 (outlining elements of trade secret misappropriation at Unif. Trade Secrets Act **§** 1(2)). Brenton also deplores the use of the CFAA in trade secret theft cases because it upsets 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 *Citrin*, gives the employer the "equivalent of a nuclear weapon." *Id. See also* Reder & O'Brien *supra* note 4, at 389 (discussing elements of proof in a trade secret claim).
[261] *See* Brenton, *supra* note 6, at 440.