FROM *MORRIS* TO *NOSAL*: THE HISTORY OF EXCEEDING AUTHORIZATION AND THE NEED FOR A CHANGE

DR. VASILEIOS KARAGIANNOPOULOS*

ABSTRACT

This Article discusses and examines the various cases that pertain to the issue of exceeding authorized access throughout the years from *United States v. Morris* to the recent *United States v. Nosal*. Further, this Article thoroughly examines the ninth circuit's approach regarding the issue of exceeding authorization; specifically, the need for the ninth circuit's narrower interpretation *United States v. Brekka* and *Nosal*. Finally, this Article proposes an alternative phrasing for the term "exceeding authorization," and a revised interpretation of the phrase and the relevant offenses under the Computer Fraud and Abuse Act. This recommended interpretation suggests establishing different degrees of authorization. In accordance with the new approach promoted by *Nosal* and Senator Lofgren's Aaron's Law Bill, this Article argues that misuses of information by authorized users should not be categorized as a computer misuse offense, but rather as a privacy law issue.

I. INTRODUCTION

Cybercrime legislation has been a peculiar area of law that was first created as a response to public fears generated by a hacker-related movie, *War Games*, before the advent of the Internet.[1] Cybercrime legislation has gotten stricter as it has expanded due to consistent political support for increased control of online activity. It seems that policy-makers have a general indifference to the practical effects of the continued increase of restrictions and penalties.[2] The primary reason for

* Dr Vasileios Karagiannopoulos is a lecturer in Socio-Legal studies at the Institute of Criminal Justice Studies, University of Portsmouth. Email: Vasileios.Karagiannopoulos@port.ac.uk

1. Reid Skibell, *Cybercrime and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 910 (2003).

2. *Id.* at 910-11.

promulgating cybercrime legislation has been the prevention of increasing damages and losses resulting from cybercrime.[3] This is consistent with policy-making on risk minimization and the prioritization of security.[4]

In the United States, the main piece of legislation that deals with computer crime is the Computer Fraud and Abuse Act (CFAA).[5] The CFAA structurally relies on the concept of authorization. Liability under the CFAA attaches only where the perpetrators, without authorization or exceeding their authorization, access or impact computers and the information contained in these computers. The Comprehensive Crime Control Act of 1984 was the legislation that preceded the CFAA that was aimed at countering computer hacking.[6] The Act did not pertain to insider misuse of information and the term "exceeding authorized access" did not exist.[7] The CFAA term "exceeding authorized access" replaces what was described in the first Act of 1984 as "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which authorization does not extend."[8]

"Unauthorized access" is undefined in the CFAA. This term relates to actions by outsiders who have no authorization to access a certain computer network and the information contained on the network yet, these outsiders manage to bypass the technical controls that prevent unauthorized users from accessing and making use of the information or the network resources. The term applicable to insiders—those who have some degree of authorization to access certain networks and information—is "exceeding authorized access." This term is defined in Section 1030(e)(6) of the CFAA: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[9] However, the concept of "exceeding authorized access" has been interpreted in different ways by courts depending upon the context of the cases.

The recent U.S. court decisions in *United States v. Brekka* and mainly *United States v. Nosal* essentially challenged pre-existing interpretations, with the aim of avoiding prosecutions of insiders under the CFAA, when there is no violation of technological restrictions. These re-

---

3. Charlotte Decker, Note, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 961 (2008).

4. *Id.*

5. 18 U.S.C. § 1030 (2010).

6. David J. Rosen, *CYBERLAW: Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access*," 27 BERKELEY TECH. L. J. 737, 744 (2012).

7. *Id.*

8. *Id.*

9. 18 U.S.C. § 1030.

cent Ninth Circuit cases have redefined the way "exceeding authorization" is perceived, in an attempt to reinstate the focus of the CFAA on computer abuse, rather than misuse of information accessed by computers or existing in them. This sounds like a logical development that is consistent with the need to employ the CFAA for the offenses it was initially created to counter and not as an all-encompassing tool for misuses of information regardless of form (i.e., electronic/computer). However, the current structure of the CFAA and prior case law pertaining to the issue of authorization might prove challenging for the new approach to be established without some major revamping of the CFAA as well. The CFAA's initial goal was to prevent computer abuse in the form of external hacking. However, later consecutive amendments to the CFAA have expanded its scope in parallel with the increasing importance of computer systems and information contained in them to protect the privacy of information and not just the integrity of the computer systems.[10] Although *Nosal* focuses on the initial goal of the CFAA, the legal system is now capable of accommodating and resolving the privacy-related risks without the need of cybercrime laws that are based on hacking.

This Article will analyse the new approach and compare the new approach to the precedent established prior to *Nosal*. Additionally, this Article will suggest a way for to structure and interpret the issue of authorization that will satisfy both the wording of the CFAA and the teleological interpretations of the CFAA as discussed in *Nosal*, and be consistent with contemporary suggestions for amending the CFAA. These discussions, based on the rationales and aims of *Nosal*, began after the broad interpretations of exceeding authorized access led to the highly aggressive prosecution, and eventually the suicide of an Internet prodigy and activist, Aaron Swartz,[11] which fuelled the already-existing discussions about the need to amend the CFAA.[12]

This Article is separated into three parts. Part II will discuss the

---

10. *See, e.g.*, 142 CONG. REC. S10,889. "[W]hile our current statute, in section 1030(a)(2) prohibits misuse of a computer to obtain information from a financial institution, it falls short of protecting the privacy and confidentiality of information on computers used in interstate or foreign commerce and communications." *Id.* "The bill would amend 1030(a)(2) to increase protection for the privacy and confidentiality of computer information . . . [t]he premise of this subsection is privacy protection." S. REP. NO. 104-357 (1996); *see* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 330-31 (2004).

11. Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, a Desperately needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 30, 2013), http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/.

12. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Acces" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1596-98 (2003) [hereinafter *Cybercrime's Scope*]; *see generally* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010) [hereinafter *Vagueness Challenges*]; Galbraith, *supra* note 10; Decker, *supra* note 3.

dominant approach pertaining to the concept of exceeding authorization, which was shaped by existing case law. Part III will discuss the cases of *Brekka* and *Nosal*, tracing the gradual development and concretization of the new approach that *Nosal* eventually established after a series of hearings. Part IV will draw some conclusions from these cases regarding the usefulness of the new approach and potential issues that might arise from its application. Part V will then discuss a new way for perceiving authorization that can lead to a more harmonious application of the *Nosal* approach. Part V will also suggest some necessary, harmonizing amendments that will aim to satisfy the concerns of the U.S. government as to the sanctioning of cases of unintended use of information, the purpose of *Nosal*, and the new CFAA bill suggested by Sen. Lofgren.[13]

II. THE ESTABLISHED APPROACH TO EXCEEDING AUTHORIZED ACCESS

A. THE "INTENDED FUNCTION" TEST

United States v. Morris established an important test for assessing the exceeding of authorized access.[14] In *Morris*, a Cornell university student created and transmitted a self-replicating, malign computer program called a "worm."[15] The worm was designed to take advantage of and highlight specific security flaws in the then-nascent Internet, exploiting program weaknesses in order for the worm to spread to multiple computers.[16] Morris was initially tried under 18 U.S.C. Section 1030(a)(5)(A), which at the time prohibited access to a "Federal interest computer" without authorization, if that access resulted in damage.[17]

Morris was convicted and then he appealed the conviction. The defendant argued that he had authorization to access several of the infected computers since many of these computers belonged to University networks that Morris had legitimate accounts at, such as Cornell, Berkeley and Harvard.[18] Morris argued that his access, regardless of whether his access was in fact unauthorized, should not be considered unauthorized. Rather, the defendant argued that his access in all in-

---

13. A bill was introduced in the U.S. Senate on June 20, 2013 to amend Title 18, United States Code, to clarify "the meaning of access without authorization, and for other purposes." Aaron's Law Act of 2013, S. 1196, 113th Cong. § 1 (2013), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-113s1196is/pdf/BILLS-113s1196is.pdf.

14. United States v. Morris, 928 F.2d 504, 506 (2d Cir. 1991).

15. Worms are self-replicating software that can infect mass numbers of computers and cause serious damage through the manipulation of existing software and data.

16. *Morris*, 928 F.2d at 506.

17. 18 U.S.C. § 1030(a)(5)(A) (2008).

18. *Morris*, 928 F.2d at 509.

stances should be considered only as instances of exceeding his given authorization, consequently absolving him from liability under Section 1030(a)(5)(A) which only required unauthorized access. In support of his argument, the defendant referenced a 1986 U.S. Senate Report that suggested a difference between "unauthorized access" and "access exceeding authorization" in relation to the difference between outsiders and insiders.[19] The former being those persons lacking any authorization whatsoever (i.e., external hackers) and the latter being those persons with some authorization to access, the limits of which they would be disregarding.[20] Consequently, according to Morris, since he was authorized to access the University computers he held accounts at and the worm originated from one these University computers, he could not be convicted of offenses relating to unauthorized access because he should be considered an insider to the network of interconnected computers.[21] Morris wanted to be considered an insider to all the computers connected to the same University network because he had access to one of those computers in the network. In other words, once a person had authorization to access one computer, this person would be considered to have authorization to access every interconnected computer on the Internet. The Second Circuit court rejected Morris' argument by stating, "Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers."[22]

With regard to the issue of exceeding authorization, the *Morris* court held that Morris exceeded his authorization when he installed the worm onto computers Morris initially had authorization to access.[23] However, where Morris installed the worm onto computers that he did not have authorization to access, his access was unauthorized because access to some federal computers did not mean that he was considered to have access to all of the federal computers that his worm eventually spread to.[24]

---

19. Kerr, *Cybercrime's Scope*, *supra* note 12, at 1630.

20. *Id.*

21. United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991).

22. *Id.* at 511 (quoting S. REP. NO. 99-432 (1986) 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488).

23. *Id.* at 510.

24. University computers could have been considered federal, yet Morris' access to such computer networks did not authorize him to access military computers, which his worm eventually reached. As the court argued, "Although the evidence may have shown that defendant's initial insertion of the worm simply exceeded his authorized access, the evidence also demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm pro-

The *Morris* court then established a new standard for determining the lack of authorization, which focused on whether the access was obtained through the use of software in intended ways.[25] The Morris court found that the programs Morris had exploited in order to allow his worm to replicate itself onto additional computers were not used in accordance with their normal function.[26] The security flaws in the software had been exploited by the defendant to facilitate access to further computers Morris lacked authorization to access, thus enabling the worm to spread further. Morris gained access via a worm program by exploiting particular software bugs that related to an unintended use of these flawed programs; therefore, his access was rendered unauthorized. Although the *Morris* court found that Morris exceeded his authorization when he installed the worm onto the computers that he was authorized to access, it is unclear whether the court reached this conclusion by applying the same "intended purpose" test it employed for assessing the lack of authorization. Regardless, it would be a safe presumption that the mere insertion of a worm into a computer that one is authorized to access would also be contradicting the intended purpose of the computer that one has been authorized to use. Further, this conduct would contradict the authorized access to the exploited software in the computers; therefore, a similar rationale could indeed be employed for assessing whether someone has exceeded his/her authorization by introducing malware or viruses into computer systems he/she was authorized to access and make normal use of.

As Orin S. Kerr discusses in a law review article, the "intended purpose" test seems to have derived from programmer community norms. These norms provide that software designers create programs to perform certain tasks and network providers implicitly authorize computer users to employ these programs to perform the tasks they were designed to operate.[27] Yet, as Kerr acknowledges, network providers would not authorize the exploitation of weaknesses in the programs in order to manipulate these programs and use them for unintended functions.[28] *Morris*, despite its importance, is a complex case regarding the distinction between unauthorized access per se and exceeding authorization. The *Morris* court was trying to prove the existence of unauthorized access through the defendant's misuse of software, rather than the exceeding of authorization for computers he was allowed to access (which was not punishable at the time). The "intended use" test of authorization will become more obvious once we examine the relevant case law that involves actual insiders.

---

gram." *Id.*

25. *Id.*
26. *Id.*
27. Kerr, *Cybercrime's Scope*, *supra* note 12, at 1632.
28. *Id.*

B. CZUBINSKI AND EXPLORICA: ESTABLISHING THE "INTENDED USE" TEST

United States v. Czubinski exemplifies the "intended function" test pertaining to insiders.[29] The defendant was an employee of the Internal Revenue Service in Boston, Massachusetts. Czubinski was authorized to access information regarding any taxpayer in the IRS computer systems via his work password.[30] IRS rules provided that employees authorized to access the IRS computer systems were not permitted to access the files held in those databases for reasons other than performing their official duties.[31] During his employment, Czubinski conducted many unauthorized searches of IRS computer files, knowingly disregarding the rules and viewing confidential information obtained by performing computer searches that were not related to his official IRS duties.[32] Czubinski's unauthorized searches involved family members, state officials and others, yet no further use had been made of that information.[33] Czubinski remained in employment until he was indicted in 1995 by a grand jury on many counts, four of which related to federal computer fraud under the CFAA Section 1030(a)(4).[34]

At the time the case was tried, the text of the computer fraud provision was:

> whoever ... knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer.[35]

The appellate court verified that Czubinski "unquestionably exceeded authorized access to a federal interest computer,"[36] because he had used his authorization to access personal information of taxpayers to satisfy his curiosity and not for his official duties.[37] However, the court found Czubinski innocent as to computer fraud because unauthorized access is a particular type of means to further a specific goal—obtaining something of value. Here, Czubinski was only satisfying his curiosity and not obtaining something of value during his unauthorized access; therefore, he was not guilty of computer fraud.[38]

---

29. *See generally* United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997).
30. *Id.* at 1071.
31. *Id.*
32. *Id.* at 1071-72.
33. *Id.* at 1072.
34. *Id.*
35. United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).
36. *Id.*
37. *Id.*
38. *Id.*

The *Czubinski* court applied a similar test as the "intended use" test in Morris for assessing the limits of authorization for insiders, based on the instructions and use policies of the employer. When the employee's use of his authorization is inconsistent with the instructions of the employer, the employee is exceeding his authorization.

In *EF Cultural Travel BV v. Explorica, Inc.*, the court discussed exceeding one's authorization in the civil context of contractual relations.[39] Although *Brekka* and *Nosal* refer to employer-employee relationships, the courts have discussed authorization as requiring a unified interpretation and these decisions have been considered important not only for employer-employee relationships, but also for cases relating to terms of use of websites and online services and whether their violation could also constitute lack or excess of authorization. This aspect of exceeding authorization was an important issue in *Brekka* and *Nosal* and will be a focal point of this Article. *Explorica* provides the majority approach regarding the interplay of website terms and conditions and unauthorized access or one's exceeding of authorization. In *Explorica*, defendant Explorica, Inc. was selling vacation packages formed by former EF Cultural Travel (EF) employees in direct competition against EF. Due to these facts, a confidentiality agreement was signed between EF and the vice president of Explorica, Inc., who was also a former employee of the former company.[40] The agreement prevented the disclosure of "technical, business, or financial information, the use or disclosure of which might reasonably be construed to be contrary to the interests of [EF]."[41]

Despite the agreement between the two companies, Explorica's head, Gormley, collaborated with Zefer, Explorica's Internet consultant, in developing a computer program that could collect all the publicly available information (Scraper) from the EF website, in facilitation of Explorica's competition with EF.[42] This program was designed specifically using technical details about the EF website in order to collect and compile information regarding the EF website that other similar programs would not be able to do with such efficiency.[43] The whole process eventually allowed Explorica to undercut EF's business and lead EF to sue Explorica for violation of the CFAA.[44]

Initially, after finding out about the Scraper program, EF requested an injunction to prevent Explorica and Zefer from using the program and demanded that all information collected through the Scraper pro-

---

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

40. *Id.* at 580.

41. *Id.* at 582.

42. *Id.* at 579.

43. *Id.*

44. *Id.* at 580.

gram be returned.[45] The district court granted a preliminary injunction against Explorica based on the CFAA, which criminally and civilly prohibits certain types of access to computers.[46] The district court found that Explorica violated the CFAA by using EF's website in ways that were beyond the reasonable expectations of EF and the ordinary uses of its website, even if the information was publicly accessible.[47]

The district court also found that EF could argue it had suffered losses due to reduced business, harm to goodwill, and the cost of employing diagnostic systems to assess possible harms to its network, yet not physical damage to EF's computers.[48] The court explained its "reasonable expectations" standard (similar to *Czubunski's* "intended use" test) and argued that the copyright indications displayed on one of the pages, the contractual obligations between Gormley and EF, which would be violated by Gormley providing information for designing the specialised Scraper, and the bypassing of technical restraints of EF's website by the Scraper, constitute adequate notifying elements for Explorica to realize that the deployment of the Scraper would be unauthorized, consequently violating the CFAA.[49]

On appeal, Explorica argued that the district court adopted an overtly narrow approach to authorization and misinterpreted the extent of the confidentiality agreement.[50] Additionally, Explorica argued that the court erred in finding that EF had suffered a loss and that the injunction was a violation of the First Amendment.[51]

Although the appellate court examined all of these issues, this Article will focus only on the appellate court's interpretation of the issues pertaining to authorization and the interpretation of exceeding authorized access, both which were considered crucial for establishing the charge of computer fraud under Section 1030(a)(4). The appellate court focused on the confidentiality agreement and concluded, "because of the broad confidentiality agreement appellants' actions 'exceed[ed] authorized access,' and so we do not reach the more general arguments made about statutory meaning, including whether use of a scraper alone renders access unauthorized."[52] The appellate court found that there was ample evidence that Gormley provided Explorica proprietary information about the structure of the website and the tour codes (which could be manually compiled in theory), but practically, "Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices

---

45. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 580 (1st Cir. 2001).
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.* at 580-81.
50. *Id.*
51. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 580-81 (1st Cir. 2001).
52. *Id.* at 581-82.

from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website."[53] Furthermore, the court discussed that the confidentiality agreement prohibited the disclosure of information that could reasonably be considered to be contradicting EF's interests. Thus, Explorica was required to prove that the use of tour codes to mine EF's pricing data was not harmful to EF's interests.[54] The court stated that if EF's allegations were proven, this would likely prove that whatever authorization Explorica had to navigate around, when accessing EF's site, it will have been exceeded by the use of specialized information and know-how in the making of the Scraper program, thus affirming the district court's view that Explorica has violated the CFAA by exceeding its authorized access.[55] In *Explorica*, the main factor that determined authorization was exceeded was the confidentiality agreement between Gormley and EF, the elements of which define the use that would be beyond the nature and the purpose of the access allowed for the general public interacting with EF's website. The "intended use" test applied in these cases is not the sole approach that preceded *Brekka* and *Nosal*.

C. *SHURGARD*, *CITRIN*, AND THE AGENCY PRINCIPLE

A civil dispute arose between competing companies in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*; this case introduced a novel approach to insider-unauthorized acts.[56] In *Shurgard*, the plaintiff argued that the defendant had attempted to lure away some of the plaintiff's employees. One such employee, Leland, who had knowledge of the plaintiff's confidential business plan and other trade secrets, emailed that information to the defendant before leaving the plaintiff's business.[57] The plaintiff sued the defendant under Section 1030(a)(2)(C) because Leland had intentionally accessed the plaintiff's computers without authorization, or by exceeding his authorization, in order to obtain the information.[58] The defendant tried to acquire a dismissal of the case arguing that Leland's access was authorized. However, the district court decided for the plaintiff, holding that authorization ceases to exist for the employees, when they start behaving in a manner that would compromise their role as agents of their original employer.[59] The basis of the court's rationale was the *Restatement (Second) of Agen-*

---

53. *Id.* at 583.

54. *Id.*

55. *Id.* at 583-84.

56. *See generally* Shurgard Storage Ctrs. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

57. *Id.* at 1123.

58. *Id.* at 1124.

59. *Id.*

cy: "[u]nless otherwise agreed, the authority of an agent is terminated, 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."[60] Consequently, the court argued that the employees, like Leland, who collaborated with the defendant "lost their authorization and were "without authorization" when they allegedly obtained and sent the proprietary information to the defendant via e-mail.[61]

Shurgard broadens the scope of liability for lack of authorization.[62] The motive of an employee while he uses his work computer determines the existence of authorization; thus, an employee could violate the CFAA for using his work computer for anything other than work-related activities.[63] The *Shurgard* perspective eliminates an employee's authorization at the moment the employee acts against his employer's interests. If the *Shurgard* analysis is used, one must consider when an employee might exceed his authorization.

For example, could an employee be liable for exceeding his authorization if he uses the work computer for personal Internet browsing even though the employer banned such use? Not likely. Although the employee goes beyond his authorization, he does not acquire adverse interests or commit serious breaches of loyalty to the principal, as per the agency principle. In order to incur liability for computer fraud under Section 1030(a)(4), or computer damage, if *Shurgard* is employed as precedent, there will not be a case where employees could exceed authorization, an approach which is at least inconsistent with the wording of the provision, requiring either exceeding authorization or lack of it.

The subsequent case of *International Airport Centers, LLC v. Citrin*[64] attempted to clarify the concept of agency and the distinction between (i) elimination of authorization as in *Shurgard* and (ii) exceeding authorization as in *Explorica*. Citrin was employed by International Airport Centers, LLC (IAC) to assist in the finding and acquisition of property, but eventually quit his job with the plaintiff and started his own business in breach of his employment contract.[65] Before leaving his employment with IAC, Citrin erased files on the laptop that IAC had provided to Citrin for his employment and rendered the files unrecoverable.[66] The erased data showed evidence of Citrin engaging in improper conduct and included files that IAC had no other copies of.[67] IAC sued under Section 1030(g) for civil compensation, arguing that Citrin had

---

60. *Id.* at 1125 (citing RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).
61. *Shurgard*, 119 F. Supp. 2d at 1125.
62. Kerr, *Cybercrime's Scope*, *supra* note 12, at 1634.
63. *Id.*
64. Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).
65. *Id.*
66. *Id.*
67. *Id.*

violated Section 1030(a)(5)(A)(i), which states "the offender knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[68] Although pressing the delete button was not considered a transmission, as per the above provision, the transmission of the secure-erase program that made the files unrecoverable was considered to fall within the scope of "transmitting a program, code or command."[69]

The court applied the principle of agency discussed in *Shurgard* and found that:

> [Citrin's] authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.[70]

The court considers the *Shurgard* case, in terms of employing the agency principle. However, at the same time the court argues that the distinction between whether Citrin had acted without authorization or by exceeding his given authorization is something that is blurry, accepting that exceeding authorization here might be a more likely interpretation.[71] The *Citrin* court discusses the concept of authorization not just in relation to the damage caused without authorization, but also in relation to the transmission of the information, which the court considers to be access.

The *Citrin* court distinguishes the facts of *Citrin* from those of *Explorica*. Although in *Explorica* access was authorized for the public in general, in the *Citrin* case, authorization solely relied on the professional relationship between the two parties. The professional relationship terminated when Citrin acted disloyally, thus voiding the agency relationship and with it the basis upon which authorization was initially given to Citrin by IAC.[72] The court does not clarify whether Citrin would have been acquitted, had it been found that he had just exceeded

---

68. *See generally id.*

69. *Id.*

70. Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

71. As the court submits:

> Muddying the picture some, the Computer Fraud and Abuse Act distinguishes between "without authorization" and "exceeding authorized access," 18 U.S.C. §§ 1030(a)(1), (2), (4), and, while making both punishable, defines the latter as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter. [internal citation omitted]. That might seem the more apt description of what Citrin did.

Id.

72. *Id.*; *see generally Explorica*, 274 F.3d 577 (1st Cir. 2001).

his authorized access. This issue of exceeding authorization as a basis for establishing the computer damage offense, despite the mention of the phrase "damage without authorization," will be of interest towards the end of this Article when the potential applicability of the changes to authorization that Nosal brings to the computer damage offense is discussed.

D. INITIAL CONCLUSIONS

In the cases aforementioned, the basis for deciding the lack of, or exceeding of, authorization is the bypassing of the purpose for which the authorization was given in the first place by somehow violating some form of private agreement, explicit or implicit, between the two parties. The combination of *Citrin, Shurgard*, and *Explorica* provides a very confusing mix of interpretations, where employees misusing employer resources and information can never exceed authorization. This can only happen when there is no duty of loyalty based on an agency relationship and when authorization does not rely on such a relationship as the sole basis. If *Czubinski's* rationale is added to the mix, the result is even more confusing, which results in three different interpretations:

1. If the duty of loyalty is breached by the employee's access, authorization is eliminated;
2. If a duty of confidentiality by an ex-employee is breached regarding access to even publicly accessible information of the employer, authorization is exceeded; and
3. If an employee violates employer policies, not for the purpose of going against the employer's interests, but rather out of plain curiosity or personal reasons, the perpetrator exceeds authorization.

Apart from the confusion generated by so many views on the issue of insider authorization, *Shurgard* and *Citrin* have another important—and probably unwanted by the legislature—consequence: an insider could also be prosecuted for reckless damage and/or negligent computer damage. In other words, a finding of breach of loyalty eliminates authorization thus rendering an insider's access equal to an outsider's unauthorized access; consequently an insider may face charges of reckless or negligent computer damage and loss. Even though these offenses were originally added to prosecute outsiders by requiring unauthorized access per se and not just exceeding authorization.[73]

The approach followed in these cases that dominate the interpretations of exceeding authorization (where someone misuses information as an employee in order to defraud his employer) assesses the given authorization to the nature of the relationship between the parties and the existence of the ulterior aim of defrauding. These cases also expand the

---

73. *See* 18 U.S.C. § 1030(a)(5)(B)–(C) (2008).

possibilities of criminalization for insiders by equating them with outsiders, even for acts that relate to misuses of information.

The problematic expansion of insider liability (the term "insider" here applies to employees and those that have authorization to access a network or website, including students accessing a university network or plain users accessing publicly accessible webpages) and the reliance on such expansion pertaining to private agreements was the focal concern in *Brekka* and *Nosal*. The Ninth Circuit attempted to resolve the issue of authorization in ways that can avoid excessively criminalizing employees and those users accessing public websites against the websites' use policies. In fact, the new approach established by the ultimate decision of the *Nosal* court, which will be discussed below, has even been integrated into a bill for amending the CFAA's concept of exceeding authorization.[74] The integration of the rationales of the *Brekka* and *Nosal* cases in a new bill makes the discussion of these cases, and mainly *Nosal*, much more pertinent in order to explore the arguments posed by the Ninth Circuit and how the final conclusion of *Nosal* was reached after an ambivalent series of rehearing and appeals. Before going into *Nosal*, *Brekka* will be briefly discussed to serve as an introduction to this new approach to exceeding authorization.

III. A NOVEL APPROACH

A. *BREKKA*

In *Brekka*, LVRC Holdings (LVRC) accused Brekka, an LVRC employee, of obtaining information; thus, engaging in unauthorized computer access and computer fraud, violating Section 1030(a)(2) and Section 1030(a)(4) respectively.[75] Brekka had access to LVRC's computers while he was employed by the company and had emailed documents to himself and his wife. The appellate court affirmed the decision of the district court, which held:

> Because Brekka was authorized to use LVRC's computers while he was employed at LVRC, he did not access a computer "without authorization" in violation of sections 1030(a)(2) or 1030(a)(4) when he emailed documents to himself and to his wife prior to leaving LVRC.

---

74. Aaron's Law Act of 2013, *supra* note 13.

75. The following is a summary of the violation(s):

> a) Whoever . . . (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . . shall be punished as provided in subsection (c) of this section.

CHARLES DOYLE, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 46 (2011).

> Nor did emailing the documents cause Brekka to "exceed authorized access," because Brekka was entitled to obtain the documents. Further, LVRC failed to establish the existence of a genuine issue of material fact as to whether Brekka accessed the LVRC website without authorization after he left the company.[76]

The district court's rationale would contradict the rationales discussed in cases mentioned earlier in this Article, where authorization would be eliminated if the employee acted against the interests of the employer. However, in *Brekka*, not only is there an elimination of authorization, which would thus establish unauthorized access, as per *Shurgard* and *Citrin*, but one could not even argue exceeding authorization by referring to *Czubinski*'s or *Explorica*'s "intended use" interpretations of authorization, even though there is obviously a breach of loyalty on behalf of Brekka.

According to the facts of the case, it was common practice for Brekka to email work-related information to his personal email during the course of his work:

> Brekka was assigned a computer at LVRC, but while commuting back and forth between Florida and Nevada, he emailed documents he obtained or created in connection with his work for LVRC to his personal computer. LVRC and Brekka did not have a written employment agreement, nor did LVRC promulgate employee guidelines that would prohibit employees from emailing LVRC documents to personal computers.[77]

Brekka had also acquired an administrative password for the LVRC website, which he later used to email information regarding LVRC to himself and his wife[78] in relation to negotiations between the defendant and LVRC.[79] Negotiations eventually broke down and Brekka left LVRC employment, handing in his work computer as well. Later, network administrators found that someone was accessing the LVRC database using Brekka's account.[80] After deactivating the account, LVRC informed the FBI that someone had accessed LVRC's network without authorization.[81]

The district court reasoned that during the time that Brekka was employed by LVRC, he had authorization to access the emails and doc-

---

76. LVRC Holdings, LCC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

77. *Id.*

78. These documents included a financial statement for the company, LVRC's marketing budget, admissions reports for patients at Fountain Ridge, and notes Brekka took from a meeting with another Nevada mental health provider. On September 4, 2003, Brekka emailed a master admissions report, which included the names of past and current patients at Fountain Ridge, to his personal email account. *Id.* at 1130.

79. *Id.* at 1129-30.

80. *Id.*

81. *Id.*

uments found on his home computer and his laptop. LVRC did not need to prove that he lacked authorization prior to leaving the company,[82] and the district court ultimately granted Brekka's motion for summary judgment.[83] Apart from the existence of authorization for Brekka to email the documents, since the company employed him, the court held that there was no evidence of a confidentiality agreement regarding the documents emailed or an explicit obligation on Brekka's behalf to return or destroy the documents upon conclusion of his LVRC employment.[84] This part of the argument seems to refer to criteria similar to *Explorica*, which LVRC could not establish as there was no explicit, written agreement of confidentiality or employee IT policy between the parties, similar to that of EF and Gormley. Moreover, the district court had found that LVRC had not produced evidence from which a reasonable jury could find that Brekka logged onto the LVRC websites after leaving employment with the company, thus dismissing all charges and claim for restitution under Section 1030(g).[85] LVRC appealed.

The appellate court addressed two issues also. First, the court focused on the existence of authorization, following the plain language of the statute.[86] Because the word "authorization" is not defined explicitly under the Act, the word should be taken to have its ordinary, contemporary meaning.[87] The court thus resorted to the dictionary definition of "authorization," defining the term as: "endorse, empower, justify, permit by or as if by some recognized or proper authority."[88] Based on this definition, the appellate court reasoned that the employer gives the employee authorization to access a company computer when the employer gives the employee permission to use the computer.[89]

LVRC argued that the court should follow the *Citrin* decision, where the employee was considered to have lost authorization when he acted against the employer's interests, breaking a duty of loyalty.[90] The court here responded that the wording of the CFAA does not support the *Citrin* approach that authorization ceases when an employee uses the computer contrary to the employer's interest. The appellate court agreed that Brekka had authorization to access the computer, as his job required such access, while Brekka was indeed still employed when he

---

82. LVRC Holdings, LCC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009).

83. *Id.*

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. WEBSTER'S THIRD INTERNATIONAL DICTIONARY 146 (2002); *see also* LVRC Holdings, LCC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).

89. *Id.*

90. *Id.* at 1134.

emailed these documents to himself and his wife.[91] The appellate court found that the application of *Citrin* to Brekka's case would consider him to be lacking authorization from the moment the information transfer to his computers from the LVRC was done with the purpose to start his own competing business, a mental state transforming him from a loyal, to a disloyal employee.[92] Instead, the court argued:

> The definition of the term "exceeds authorized access" from § 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer. The plain language of the statute therefore indicates that "exceeding authorization" depends on actions taken by the employer to pose explicit limitations on the use of the authorization given to his/her employees. Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer.[93]

The court reached this conclusion to avoid a more abstract interpretation, arguing that it could not interpret criminal statutes in surprising ways that could impose unanticipated penalties on the defendants.[94] Consequently, the court submitted that, unless the employer had actually taken steps to revoke the employee's authorization, Brekka would have no way of knowing he lacked authorization. There was no explicit use policy that prevented Brekka from acting as he did (in fact he was emailing himself work documents for work purposes all the time) and thus, he could not be found guilty of the said CFAA offenses, just because his behavior was in breach of a fiduciary duty to an employer.[95]

At the same time, the question naturally arising from the rationale of the *Brekka* court, which required explicit revocation of authorization, is, of course, how could the employer revoke authorization, when he is not aware of any existing reason to do so? Brekka had not made his intentions known to his employer before the file transfer. In addition, the same argument may be valid for other similar cases of disloyal employees who will seek to take advantage of their authorization against their employers without the employers having any knowledge of their employees' discrepancies, so as to revoke the authorization.

Moreover, another question is whether Brekka was indeed unaware that he would be exceeding his authorization while so obviously

---

91. *Id.* at 1133.

92. *Id.* at 1134.

93. *Id.* at 1135.

94. LVRC Holdings, LCC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009); *see* United States v. Santos, 128 S.Ct. 2020, 2025 (2008) (plurality opinion) (citing United States v. Bass, 404 U.S. 336, 347-49 (1971); McBoyle v. United States, 283 U.S. 25, 27 (1931); United States v. Gradwell, 243 U.S. 476, 485 (1917)).

95. *Brekka*, 581 F.3d at 1135.

acting against his employer's interests. Since it could be reasonably construed that, if the employer knew that authorization was being used in order to support a competing business or undermine its interests more generally, the employer would most probably rescind the employee's authorization. Would it then be a surprise for Brekka to lose his authorization if his use of authorization for unintended purposes was uncovered? Probably not. Nevertheless, the court seems to have avoided such questions. The case of *United States v. Nosal*, however, broadened this interpretation and resolved such issues.

B. THE *NOSAL* ODYSSEY

Nosal also relates to employees collaborating against their employer, but the implications and discussion in the case went even further to discuss authorization in the sense of users violating terms and conditions of websites.

Nosal worked as an executive for a company called Korn/Ferry International, an executive search firm. When Nosal left the company, he signed a Separation and General Release Agreement and an independent Contractor Agreement.[96] Pursuant to these agreements, Nosal agreed to serve as an independent contractor and to avoid competing with his former employees for a year in exchange for some pecuniary compensation.[97] Shortly after leaving, Nosal approached three other employees of Korn/Ferry in order to convince them to help him set up a competing business.[98] These three employees allegedly obtained trade secrets and other proprietary information through their accounts, which allowed them access to the Korn/Ferry network. Then, they transferred to Nosal information coming from the Searcher database of Korn/Ferry, which was considered a highly confidential, proprietary, global database of executives and companies.[99]

Korn/Ferry actually took extensive measures to secure its database, as was documented during the hearings, by controlling electronic and physical access to it.[100] For example, each Korn/Ferry employee was assigned a specific username and password to use in order to access the database, making sure only employees could access the database.[101] Furthermore, the company required its employees to sign an agreement that both explained the confidential, proprietary nature of the Searcher database and restricted the use of all information in it, except for legit-

---

96. United States v. Nosal, 642 F.3d 781, 782 (9th Cir. 2011) [hereinafter *Nosal I*].
97. *Id.*
98. *Id.* at 783.
99. *Id.*
100. *Id.*
101. *Id.*

imate company business.[102] Korn/Ferry further declared the confidentiality of the information by stamping reports using information from that database with the phrase: "Korn/Ferry Proprietary and Confidential."[103] Finally, upon accessing the company computer system, the accessor was met with a notification, highlighting the proprietary nature of the information in the database and the need for specific authorization from the company for accessing the database, the lack of which could lead to disciplinary action or criminal prosecution.[104]

The *Nosal* case relates to charges of a computer fraud under Section 1030(a)(4) (among other non-CFAA offenses that are irrelevant here for the discussion of authorization), alleging that Nosal's co-conspirators had exceeded their authorization to access the Korn/Ferry computers.[105] This was done by obtaining information from their employer's computers for the purpose of defrauding Korn/Ferry and assisting Nosal in setting up his competing business.[106]

For purposes of discussion in this Article, the initial hearings will be identified as *Nosal 1*. After the first round of hearings, the case went through a second round of hearings, identified herein as *Nosal 2* that eventually produced an opposite final conclusion from that of *Nosal 1*.

1. United States v. Nosal: The First Stage (2011) ("*Nosal 1*")

Initially, the government filed an indictment against Nosal and one of his accomplices for violation of the computer fraud provision, pursuant to Section 1030(a)(4)—Nosal being an aider and abettor.[107] Nosal argued that the indictment should be dismissed since employees could not have accessed that information without prior authorization, or by exceeding their given authorization, because they had permission to access that information under certain circumstances.[108] He argued that the CFAA did not cover employees misappropriating information or violating confidentiality agreements by using information of the employer in a manner that was breaching those private agreements.[109]

The district court initially dismissed Nosal's arguments regarding authorization; yet, Nosal filed a motion to reconsider once Brekka was decided, which refined the concepts of lack of authorization and exceeding authorization.[110] The District Court agreed with Nosal during that second hearing, being compelled by *Brekka*, to accept that:

---

102. *Nosal 1*, 642 F.3d 781, 783 (9th Cir. 2011).
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*
108. *Nosal 1*, 642 F.3d 781, 783 (9th Cir. 2011).
109. *Id.*
110. *Id.*

> the phrase "exceeds authorized access" as used in the CFAA means having permission to access a portion of a computer (or certain information on a computer), but accessing a different portion of the computer (or different information on the computer) that the employee is not entitled to access under any circumstances.[111]

The court's discussion not only links exceeding authorization to the existence of some prior authorization, but also to the bypassing of technical restrictions for accessing a network the employer is not authorized to access.

The district court also stated that intent was not relevant in order to determine whether someone exceeds authorized access, even if an employee's access to the computer is expressly limited by the employer's use restrictions.[112] The district court's view is contrary to the "intended use" test of *Morris* and *Czubinski* and the agency principle in *Shurgard* and *Citrin*. Consequently, since Nosal's conspirators had access to the information obtained, having remained employees of Korn/Ferry, the court did not consider their access as being in excess of authorization, despite the existence of obvious fraudulent intent. Thus, the defendants were considered not guilty of violating Section 1030(a)(4), with the government appealing that decision.[113]

2. *Nosal 1* Appellate Court

The appellate court reviewed the case *de novo*, focusing on the question of whether Nosal's accomplishes had exceeded their authorization.[114] At first, the appellate court assessed the wording of "exceeding authorized access" which reads: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[115]

The government focused on the word "so," arguing that Nosal's interpretation would render the word superfluous, and further added that "so" means "in a manner or way that is indicated or suggested."[116] Therefore, according to the government's interpretation, an employee would exceed authorization when using his authorized access to obtain or alter information that he is not entitled to obtain or alter in the manner that he does.[117] Thus, the government argued that its interpretation of "exceeding authorization" was similar to the "intended use" test and consistent with the basic rule that statutes must be interpreted

---

111. *Id.* at 784.
112. *Id.*
113. *Id.* at 785.
114. *Nosal 1*, 642 F.3d 781, 785 (9th Cir. 2011).
115. § 1030(e)(6).
116. *Nosal 1*, 642 F.3d at 785.
117. *Id.* at 786.

in such a way, so that no part remains inoperative, superfluous, void, or insignificant.[118]

Next, the appellate court evaluated Nosal's argument that the decision of *Brekka* nullifies the government's interpretation mentioned above for "exceeding authorized access."[119] The appellate court argued that *Brekka* had decided that the crucial element for assessing whether authorization has been exceeded was not the motive of the employee and his violation of the interests of the employer, as it would be with *Citrin*, but rather the explicit action by the employer revoking authorization.[120] The appellate court voiced its concern about the inability of the employee to know that authorization had been revoked without the existence of an explicit revocation from the employer. This concern motivated the court to apply the rule of lenity "which is rooted in consideration of notice and requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government" and opt for the more restricted interpretation of exceeding authorized access.[121] Consequently, since Brekka had not been notified of any restrictions to his access, nor had any way of knowing whether or when the employer might have revoked his authorization, he was still authorized to access the computer he did, even for fraudulent purposes.[122]

The appellate court then argued that its decision that an employer's use restrictions define whether employees have exceeded their authorization is an application of the above *Brekka* rationale that bases the existence of authorization on the acts of the employer to revoke the authorization given. Therefore, according to this rationale, the only logical interpretation of "exceeding authorized access" would be that the employer has placed limitations on the employees' permission to use the computer and they have violated those limitations.[123]

The major difference between *Brekka* and *Nosal* is that Brekka had unrestricted access to the company computer and there were no written employment agreement or employee guidelines in order to explicitly prohibit employees from emailing LVRC documents for personal use to personal computers. Based on these facts, Brekka had not violated any established access restrictions; therefore, his access was not exceeding authorization.[124] However, in the case of *Nosal*, Korn/Ferry had imposed a detailed computer use policy for its employees that entailed clear and explicit restrictions on the employees' access to both the net-

---

118. *See* Corley v. United States, 556 U.S. 303, 313 (2009).
119. *Id.*
120. *Nosal 1*, 642 F.3d 781, 786 (9th Cir. 2011).
121. *Id.* at 786-87 (citing United States v. Romm, 455 F.3d 990, 1001 (9th Cir. 2006)).
122. *Id.* at 787.
123. *Id.*
124. *Id.*

work and the Searcher database.[125] Therefore, the employees that were collaborating with Nosal, and then using their authorization to access their employer's resources in order to defraud Korn/Ferry in violation of the company's access restrictions, were considered to have a fair warning regarding their potential liability for unauthorized access.[126] Therefore, the rule of lenity could not exonerate the offenders from liability, as with *Brekka*.[127] The court argued that Nosal's concerns about the government's broad interpretation of exceeding authorization that could criminalize activities of employees depending on the whims of employers are eliminated by the *Brekka* decision.[128] The *Brekka* decision stated that the employer can determine whether an employee is acting in an authorized manner, as long as the employee has explicit knowledge of the employer's limitations to his/her authorization.[129]

The *Nosal 1* court also referred to other circuits having addressed the issue. It mentioned *United States v. John*, in which the court argued that when the user knows or reasonably should know that he is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime, the user is subject to prosecution under the CFAA.[130] In this case, the employee had accessed confidential information in violation of the employer's computer use restrictions.[131] Similarly, the Eleventh Circuit in *United States v. Rodriguez* followed the *Brekka* rationale, arguing that an employee of the Social Security Administration that made use of his authorized access to obtain information for personal reasons had exceeded authorization.[132] Unlike the *Brekka* case, the Administration had told Rodriguez that he was not authorized to use personal information he could access at work for personal reasons.[133]

Based on the above, the appellate court of *Nosal 1* reversed the decision of the district court, which had found that Nosal and his accomplices had not exceeded their authorization.[134] Furthermore, the appellate court allayed concerns that its interpretation of exceeding authorization, as reliant on the employer's explicit use policies and actions would criminalize employees checking sports scores or personal email accounts through their work computers.[135] The court argued that simply using a work computer in violation of the employer's restrictions

---

125. *Id.*
126. *Nosal 1*, 642 F.3d 781, 787-88 (9th Cir. 2011).
127. *Id.* at 787-88.
128. *Id.* at 788.
129. *Id.*
130. United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).
131. *Id.*
132. United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).
133. *Id.*
134. *Nosal 1*, 642 F.3d 781, 789 (9th Cir. 2011).
135. *Id.* at 788.

is not a crime under Section 1030(a)(4) since an intent to defraud and the obtainment of something of value through that access is also required.[136]

Yet that would not be the end of the *Nosal* case. Although the above decisions seemed to have finally resolved the issue somewhere in between the intended test function and what Nosal was arguing, eventually, the Ninth Circuit court decided to rehear the case *en banc*. The court subsequently ended up affirming the very first decision of the district court, which the first decisions of the appellate court in 2011 (*Nosal 1*) had reversed. In Nosal 2, the Ninth Circuit found that the violation of employer computer use policies and terms of use of private websites, implicit or explicit, could not be the basis for deciding on the lack or the exceeding of authorization.[137]

3. United States v. Nosal (2012) ("*Nosal 2*")

In *Nosal 1*, the district court had initially rejected Nosal's arguments regarding the inapplicability of offenses that related to exceeding authorized access to his case.[138] After *Brekka* was decided and in light of the interpretations introduced by *Brekka* regarding exceeding authorization, the district court had reheard the case, reversing its initial view to agree with *Brekka* and to consider that there had not been any case of unauthorized access or exceeding authorization.[139]

The discussion in the *en banc* appellate hearing of the *Nosal 2* focused anew on the issue of exceeding authorized access and the two potential readings of the definition of Section 1030(e)(6).[140] First, according to the defendant, exceeding authorization refers to a person that has authorization to access only certain data or files and accesses data or files that he is not authorized to, something known as hacking.[141] The second interpretation, which the government has provided to "exceeding authorized access" and which relates to the above concern, is that the language of exceeding authorization could refer to a person that has unrestricted physical access to a computer network, but is restricted through employment contracts or computer-use policies in the use of the information he is technically able to access.[142] The example here is that an employee is allowed to access customer lists for doing his job, but not

---

136. *Id.* at 788-89 (9th Cir. 2011).

137. *See generally* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) [hereinafter *Nosal 2*].

138. *Nosal 1*, 642 F.3d at 784.

139. *See* LVRC Holdings, LCC v. Brekka, 581 F.3d 1127, 1127 (9th Cir. 2009).

140. *Nosal 2*, 676 F.3d at 856.

141. The court provides the example of an employee having access authorization in relation to product information on the company's network, yet she accesses customer data, which would render her access excessive. *Id.* at 860.

142. *Id.*

to send them to a competitor,[143] which is essentially the rationale followed in *Czubinski*.[144]

Next, the appellate court discussed the suggestions regarding the term "entitled" and its meaning in the phrase: "an accesser is not entitled so to obtain or alter."[145] The government pointed to a dictionary definition of "entitle" interpreted as "to furnish with a right."[146] Based on that definition, the government argued that Korn/Ferry's use policies for its computer network provided certain rights to the employees, and when employees violated those policies, they exceeded their authorization by going beyond their given rights.[147]

The court, however, argued that the word "entitled" relates to how an accesser obtains or alters the information and argued that the more sensible interpretation to be followed regarding the term "entitled" would be to consider it a synonym for "authorized."[148] If read like this, "exceeding authorization" would refer to data or files on a computer that the employee is not authorized to access.[149]

Regarding this argument, one cannot help but wonder why the legislature would use two different words if they were meant to signify exactly the same use? An alternative interpretation will be discussed later in this Article when discussing the potential alternative interpretations for revamping the notion of authorization according to *Nosal*.

Next, the court discussed the governmental interpretation of the term "so" in the phrase above.[150] The government read "so" to mean "in that manner," which it claimed must relate to computer use policies and restrictions, since a narrower interpretation would render "so" superfluous.[151] The court argued that the interpretation of "so" in such a way would turn the CFAA from an anti-hacking statute into an expansive misappropriation statute, placing too much attention on a two-letter word.[152] As the court further argued, if Congress meant to expand the CFAA to criminalize everyone that uses a computer in violation of computer use restrictions, it is expected to use more appropriate and explicit wording in order to achieve this result.[153] The court also provided examples that attempt to interpret the reason for inserting "so" in the sentence, but argues that it is not clear whether the state might have

---

143. *Nosal 2*, 676 F.3d 854, 860 (9th Cir. 2012).
144. *See generally* United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997).
145. *Nosal 2*, 676 F.3d at 857.
146. *Id.* (citing to WEBSTER'S NEW RIVERSIDE UNIVERSITY DICTIONARY 435 (1984)).
147. *Nosal 2*, 676 F.3d at 857; *Nosal 1*, 642 F.3d 781, 787 (9th Cir. 2011).
148. *Nosal 2*, 676 F.3d at 857.
149. *Nosal 2*, 676 F.3d 854, 857 (9th Cir. 2012).
150. *Id.* at 863.
151. *Id.*
152. *Id.* at 854.
153. *Id.* at 857.

just put the word in as a connector or for emphasis instead of doing it for a substantive reason.[154]

Eventually, the court agreed with Nosal's narrower interpretation of the CFAA, considering the CFAA an act that relates to penalizing hacking and not computer use policy violations.[155] The court stated that since the CFAA was meant to deal with hacking, it contained the term "unauthorized access" for bypassing technological controls.[156] That means, according to the government, that exceeding authorization relates to users who already have authorization yet use it for unauthorized purposes, as in *Czubinski*.[157] Yet for the court, the above construction by the government would end up criminalizing any unauthorized use (not only in the technological sense here) of information under the CFAA only because it was obtained from a computer. It is highly unlikely to have been what Congress meant, as it goes well beyond the purpose of breaking into a computer.[158] The court further provided historical evidence regarding the concept of exceeding authorized access that supported its approach to avoid criminalizing an employee for the illegitimate use of data.[159]

Before proceeding to analyze the conclusions from the *Nosal* cases and the alternative approach that will be suggested later in this Article regarding authorization, it is useful to see how the court justified its rationale for wanting to avoid criminalization under the CFAA based on violating terms of use and employer policies and stick solely to breaking into computers. The court focused on the fact that criminalizing casual violations of computer-use policies, such as chatting with friends or playing games, could become federal crimes if the government's interpretation of exceeding authorization is accepted.[160] As the court argues, enforcement of the CFAA against employees has indeed happened; therefore, the threat of expanding the CFAA in the way suggested by the government should be considered seriously.[161] Prosecutors should not even have the legal tools available for resorting to ridiculous prosecutions, for example, by prosecuting users for violating terms and conditions of websites under the premise of exceeding authorization.

---

154. *Id.* at 858; *Nosal 1*, 642 F.3d 781, 788-89 (9th Cir. 2011).

155. *Nosal 2*, 676 F.3d 854, 858 (9th Cir. 2012).

156. *Id.*

157. *Id.*

158. *Id.* at 859.

159. Rosen, *supra* note 6.

160. *Nosal 2*, 676 F.3d at 860.

161. *Nosal 2*, 676 F.3d 854, 860 (9th Cir. 2012). The court mentions the case Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011) (holding that where an employer sued for unlawful termination had counterclaimed that the plaintiff violated section 1030(a)(2)(C) by using the Internet for personal reasons, yet the district court dismissed the claim based on the rationale that exceeding authorization did not include violating private computer use policies). *Id.* at 860 n. 6.

The court argued that employer-employee and company-consumer relationships are usually regulated by tort and contract law. The governmental view would result in these relationships being manipulated by private parties in order to police them through criminal law.[162] Furthermore, the court questions the vagueness of the limit between a prosecutable and non-prosecutable business purpose, giving examples of many innocuous offline behaviors at work that, when transposed online, would constitute criminal offenses based on exceeding authorized use of the work computers or even terms of service of popular websites, such as Google, Facebook or even dating sites.[163] The court expressed its concern that attaching felonious liability for CFAA offenses due to an alleged violation of vague and unknown or arbitrarily changeable Terms of Service could prove very dangerous for millions of plain users.[164] The fact that the government assures it would not prosecute such types of exceeding authorization is not reason for accepting its interpretation, since the discretion of prosecutors should not be relied upon.[165]

The court mentions that such governmental guarantees are not to be trusted, citing the example of *United States v. Drew*. In the *Drew* case, the prosecutor decided to press charges against defendant Drew, who created a fake Myspace account in order to bully her daughter's friend online.[166] Unfortunately, the bullied victim committed suicide.[167] The input of fake information on Myspace on behalf of Drew in order to create an account on MySpace as posing as a young boy was in violation of the terms of use of the website.[168] Based on that fact, the prosecutor brought charges against Drew for obtaining information from a protected computer by exceeding authorized access.[169] The rationale is that Drew was authorized to use Myspace as an adult user putting in her actual personal information, but was in breach of Myspace's terms of use when she created the fake account.[170] According to the prosecutor, Drew exceeded her authorization to use Myspace.[171] Drew was initially convicted by the jury for a CFAA misdemeanour violation, but that decision was overturned by the judge after Drew filed a motion for acquittal.[172]

---

162. *Nosal 2*, 676 F.3d at 860.
163. *Id.* at 861-62.
164. *Id.* at 862.
165. *Id.*
166. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).
167. *Id.*
168. *Id.*
169. *Nosal 2*, 676 F.3d 854, 862 (9th Cir. 2012); *see Drew*, 259 F.R.D. at 452 (holding where a mother that cyberbullied her daughter's classmate through a fake profile on MySpace was charged with § 1030 (a)(2)(C) for violating the terms of service, which required the input of truthful identifying information).
170. *Drew*, 259 F.R.D. at 452.
171. *Id.*
172. United States v. Drew, 259 F.R.D. 449, 451 (C.D. Cal. 2009).

The judge accepted that allowing CFAA prosecutions to be based on the violation of terms of use as exceeding authorized access would render the statute void for vagueness due to a lack of sufficient notice to the public regarding such violations and lack of proper prosecutorial guidance on the issue.[173] The *Nosal 2* court mentions this example in order to demonstrate how, despite the government's assurances regarding exaggerated prosecutions, some prosecutors might give in to political pressures, such as those generated by the suicide of the victim in the *Drew* case.[174]

On the same note, the *Nosal 2* court also quotes the *United States* v. *Kozminski*,[175] where the court argued that the governmental interpretation of exceeding authorization would "delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crime'" and would "subject individuals to the risk of arbitrary or discriminatory prosecution and conviction."[176] Based on these concerns, *Nosal 2*, unsurprisingly, decided to follow *Brekka* and the other courts having reached similar conclusions, regarding the criminalization of unauthorized access to information and not its misuse.[177] Consequently, the court found Nosal and his accomplices, who had access to the company's databases, could not be charged with computer fraud as they did not lack, nor had they exceeded authorization, accepting that the government could prosecute for the rest of the counts of the indictment apart from the CFAA-related ones.[178]

Nosal has been a crucial case regarding talks about narrowing down the scope of the CFAA, yet the different circuits in the United States have been split regarding the interpretation of exceeding authorization.

---

173. *Id.* at 464.

174. *Nosal 2*, 676 F.3d 854, 862 (9th Cir. 2012).

175. United States v. Kozminski, 487 U.S. 931, 932 (1988).

176. The *Nosal* court rejected the rationales adopted by other circuits such as those having identified breaches of corporate computer use restrictions or violations of a duty of loyalty to be within the scope of CFAA. Instead, it urged these courts to reconsider and criticized their indifference to the potential consequences of their adoption of such broad interpretations of the CFAA for regular employees and Internet users. *See, e.g.,* Rodriguez, 628 F.3d 1258 (2010); United States v. John, 597 F.3d 263 (2010); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); *Nosal 2*, 676 F.3d at 870-71.

177. *Nosal 2*, 676 F.3d at 854 (citing e.g. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005)).

178. *Nosal 2*, 676 F.3d at 864.

IV. THOUGHTS AND CONCERNS *NOSAL* GENERATES

A. *NOSAL 2* HARMONIZES ALL THE OFFENSES OF THE CFAA

The *Nosal 2* court made an effort to remedy the problem of having different standards for exceeding authorization across different provisions of the same Act. As the court argued, the interpretation of the government's argument regarding exceeding authorization is even more problematic since the concept of "exceeding authorized access" exists in other offenses apart from computer fraud, Section 1030(a)(4).[179] For example, in Section 1030(a)(2), "exceeding authorized access" is used to obtain information from a protected computer. The broad interpretation that has been attributed to the "protected computer" potentially includes every computer online,[180] essentially making every violation of a private use policy online on a global scale a federal offense.[181]

Consequently, the clarification that liability for exceeding authorization cannot rely on private terms and conditions or employer use policies is initially important in order to solidify the elements of liability and to reduce the chances where users could be prosecuted for CFAA offences in general, based on private agreements. What makes the rationale followed by the *Nosal 2* court regarding "exceeding authorization" even more pertinent here and demonstrates a disparity in the treatment of the different types of insiders is the exclusion of federal employees from exceeding authorization, when accessing non-public, federal computers, an offense described in Section 1030(a)(3).[182]

Congress has eliminated the possibility of insiders/governmental employees being prosecuted under the unauthorized access to federal computers offense (Section 1030(a)(3)) for accessing computers in their

---

179. *Id.* at 863.

180. Initially "protected computer" was defined as a computer "used by the federal government or a financial institution" or one "which is used in interstate or foreign commerce." The current, considerably broader defines a protected computer as "a computer (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2) (2008).

181. *Nosal 2*, 676 F.3d 854, 854 (9th Cir. 2012).

182. 18 U.S.C. § 1030 states as follows:

> (a) whoever . . . (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

18 U.S.C. § 1030.

own department, where they are authorized to access non-public computers in the course of their duties, by not including the concept of "exceeding authorized access" in the wording of this provision, thus making it applicable only to outsiders.[183] The purpose was to avoid criminalizing insiders for exceeding their authorization to view information within their department. The Committee felt that looking at information in one's own department, where one has authorization to access the information technologically through a password, but would not be entitled to do so actually—in relation to the nature of his duties—should not be considered criminal, and administrative penalties would be more appropriate.[184]

Although Congress adopted the view that prosecutions of insiders should be avoided regarding the use of information they are authorized to access in their department, despite not having the right to do so as far as their duties are concerned, it has decided to preserve exceeding authorized access as part of the actus reus of other offenses relating to the CFAA. However, similar disputes and problems of excessive criminalization of insiders have consistently arisen in the private sector, under Section 1030(a)(2) that relates to obtaining information (obtaining can be merely looking, as seen above, with no further need for use of that information for malign purposes) from protected computers.[185] The comparison here is made between Section 1030(a)(2) and Section 1030(a)(3) because these sections are the only sections criminalizing the plain obtainment of information without any further malign intent.

In the case of Section 1030(a)(3), the State sought to protect its own employees from the liability excesses that the vagueness of the term "exceeding authorized access" could cause. But it was not as sensitive regarding insiders/employees in the private sector, allowing for a vague term to remain throughout many amendments and failing to provide a resolution to the issue despite the continuing and expanding conflict between the various circuits. Congress has, of course, retained the criminalization of interdepartmental unauthorized access, even regarding Section 1030(a)(3), in order to avoid allowing public servants with authorization to access certain governmental computers to plead that

---

183. *Id.*

184. DOYLE, *supra* note 75, at 3-4.

185. 18 U.S.C. § 1030 states as follows:

> (a) Whoever (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act 15 U.S.C. 1681 et seq.);
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer.

18 U.S.C. § 1030.

they were actually insiders to every non-public governmental computer. Different departments with obviously different passwords and computer systems would require the bypassing of technological authorization controls and that would render even federal employees liable for unauthorized use. In general, it would appear that intra-departmentally, lack of authorization that could amount to criminal charges cannot be constituted. Interdepartmental unauthorized access, however, for Section 1030(a)(3) is equated to outsider access, since it would also probably entail the bypassing of technological controls.

The court in *Nosal 2* attempts to potentially remedy this disparity between Section 1030(a)(2) and Section 1030(a)(3) for insiders by rendering "exceeding authorized access" inapplicable to all those having some sort of authorization based on a private agreement or terms of use, such as plain users or employees accessing their workplace computers just to get information for personal reasons. *Nosal* seems to be drawing the same analogy for insiders, such as employees accessing information of a private company where they work. According to *Nosal 2,* if the employees have authorization in terms of technological access, they cannot be considered to be accessing without authorization or by exceeding it and, thus, are in no way prosecutable for it, under the CFAA, based solely on violations of terms of use or employer policies. If employees do not have technological access to parts of a network they are generally authorized to access, they are equal to outsiders for the specific part of network or information and, therefore, any bypassing of the technological controls and access to the information that was normally out of bounds is unauthorized access and not in excess of authorization, since the technologically non-accessible part of a network is in essence an independent sub-network, that might be part of a network the person is normally authorized to access. However, it still is, or should be, considered independent in terms of accessibility; therefore, access to it should also be treated independently in terms of authorization.

Such a rationale could easily be expanded to insiders and employees of other sectors where there exist protected computers in order to avoid unjust and irrelevant charges under the CFAA for insiders.

B. Exceeding Becomes Even More Obsolete

The harmonization discussed above essentially demonstrates the potential obsoleteness of the concept of "exceeding authorization" in its current form and conception, a conclusion we can draw not only from the decision in *Nosal 2*, but also from previous cases, which also extensively limited the scope of the term "exceeding authorization." *Shurgard* and *Citrin* limited the applicability of "exceeding authorization" to employee-related cases by finding insider misuses of authorization to be

eliminating authorization, rather than exceeding it. This was held to be true even if it could be argued that this would be the case only where the employee made use of his authorization in ways not just unintended, but in ways that proved a disloyal behavior towards the employer that had given the authorization. This Article suggests employing the rationale of *Czubinski* in cases where the use was unintended, such as private collection of information due to curiosity, but not harmful to the employer or for cases like *Explorica* where private confidentiality agreements could indicate that the use of existing authorization was going beyond the intended limits that authorization was allowed.

However, the use of the term in computer fraud regarding employees would definitely be compromised. In those cases, either *Nosal 2* would have to be employed (denying that authorization has been exceeded) or *Shurgard*/*Citrin* would have to be used (accepting that authorization has been eliminated). Actually, *Nosal 2* eliminates all the potential instances that are based on private agreements of computer use policies and terms of use or fiduciary duties of employees towards employers. This would eliminate the application of any standard discussed so far for exceeding authorization, be it intended use in *Czubinski,* breach of loyalty in *Shurgard* and *Citrin,* or even the vague *Brekka* standard requiring explicit, prescribed employer computer use policies for defining whether authorization has been exceeded.

Nosal 2 requires that CFAA liability that is based on exceeding authorized access relate only to cases of violations of technological restrictions. Yet, if there are technological restrictions even for insiders, it is questionable whether they would be considered insiders practically. In this situation, those that have some sort of authorization to access a certain network would have to be defined as insiders, but no authorization to access another part of the same network. However, this distinction does not seem to support any practical difference between insiders and outsiders, apart from the fact that the alleged insiders have a preexisting link—but not full access—to the network they eventually access beyond the limits of their given authorization. Since both outsiders and the limited-authorization insiders have to bypass technological restrictions to access the information in question, they both eventually exceed their given authorizations. The fact that insiders might have some type of authorization for other files in the same network does not seem to make that much of a difference legally regarding sanctions. There is no specific provision relating to lesser or higher penalties for insiders than outsiders. The potential differentiation could be that taking advantage of a position of trust as is provided in the United States Sentencing Guidelines Section 3B1.3 (abuse of position of trust or use of special skill): the defendant abused a position of public or private trust [. . .] in a manner that significantly facilitated the commission or con-

cealment of the offense.[186] If insiders are often considered to be in a position of trust compared to outsiders, the distinction might be meaningful as it would raise the count by two levels.[187] However, the tendency of the legislature to want to avoid insider punishment for federal employees would imply that perhaps in cases of access to information that are not part of the employee's official duties, the penalties would be more lenient rather than stricter as a means of highlighting the relationship of trust that exists between employers-employees. Consequently, since the fact that someone violates the CFAA as an insider rather than an outsider does not entail a difference in liability and penalties, the need for the use of the term of "exceeding authorization" becomes practically obsolete. The employment of the aforementioned sentencing guidelines could be supported by the examination of the facts of the case without the need for different terminology in the wording of the actual offense.

Seeing that many different judicial interpretations of the issue of "exceeding authorization" have been so restrictive to the applicability of the term, one can argue that this term might have become obsolete over the years or even dangerously applicable to inappropriate cases. Such cases include those described in *Nosal 2* above regarding website terms and conditions[188] and whether the term "exceeding authorization" could be substituted by employing a different wording. A different wording could realize the purpose of the CFAA more consistently to protect from computer misuses while eliminating the instances it could be misapplied to incidents that relate to privately agreed or imposed restrictions on the use of accessible information.

V. A NEW TERMINOLOGICAL APPROACH TO EXCEEDING AUTHORIZATION

A. FRAGMENTING UNAUTHORIZED ACCESS AND SUBSTITUTING EXCEEDING AUTHORIZATION WITH ENTITLEMENT

The conflict between the government and the court in *Nosal 2* potentially flows from the perception of authorization as one all-encompassing permit. This view is reinforced by the interpretation of "entitled," in the definition of exceeding authorization, as "author-

---

186. United States Sentencing Commission, '2011 Federal Sentencing Guidelines Manual' Chapter 3 available at <http://www.ussc.gov/Guidelines/2011_Guidelines/Manual_PDF/index.cfm>

187. The potential differentiation could be that taking advantage of a position of trust as is provided in the US Sentencing Guidelines Section 3B1.3 (Abuse of position of trust or use of special skill): the defendant abused a position of public or private trust [...]in a manner that significantly facilitated the commission or concealment of the offence. If we consider that insiders will often be in a position of trust compares to outsiders the distinction might be meaningful, as it would raise the count by two levels. *Id*

188. *Nosal 2*, 676 F.3d 854, 859 (9th Cir. 2012).

ized."[189] An alternative wording that may lead to a clearer interpretation for lacking or exceeding authorization could be the separation of authorization and entitlement as two different concepts, each applicable to different conditions. For example, the notion of authorization will be strictly linked to technological permits or restrictions and will be fragmented into different types of authorized use for different uses of information in computer systems. This way there would be no "exceeding authorization" even for insiders having some level of authorized use, but just different levels of authorization that, if violated, would result in unauthorized use, the same way as we now perceive it for outsiders. Insiders will not be able to violate the CFAA within their sphere of technologically authorized use. However, those insiders lacking some aspect of authorization would be prosecutable under the CFAA, when they violate the technical restrictions limiting their extent of authorization. This approach would of course be consistent with the decision in *Nosal 2* regarding the concept of exceeding authorization and the need for violating technical restrictions.

For example, under this suggested method, an employee could be authorized to view (access) the information, but unauthorized to copy. We could consider accessing/viewing as the basic use level that one could be authorized to have, perhaps in the form of a password to access the network and view information. This would also cover, apart from employees, the basic access that relates to users browsing websites or using online services, such as Myspace or sport websites. Since access immediately allows us to view information and because merely viewing it is analagous to obtaining the said information, access could be established as an initial type of use. Other types of use, such as downloading, copying, sharing or modifying could be prohibited. Authorization could be defined in terms of someone having the technological permit allowing certain uses of information, from viewing to deleting. If one bypassed technological controls and modified the information he was not authorized to modify, even though he had access to view the information, he would have acted without authorization and exceeding his authorization, because his copying would be unauthorized.

The term "exceeding authorized access" seems like a contradiction in terms, if we accept the interpretation of *Nosal 2* that requires the bypassing of technological controls in order for insiders to exceed authorization, simultaneously disregarding the interpretation that focuses on unauthorized use of authorized access, as in *Czubinski*. If technological restrictions have to be bypassed in order for "exceeding authorized access" to be perpetrated by insiders, it can be argued that by instituting different levels of authorization, one could just claim that someone has

189. *See supra* Section III.B.3.

used information in an unauthorized way, even if he has authorization for certain types of use (viewing, but not modifying for example) and avoid the confusing double standard of exceeding and lacking authorization. If authorization is perceived as related to a technological permit to certain uses of information, one either has authorization to use information in a specific way through his user codes and passwords, or does not. For example, deciding to crack a security code preventing employee access to certain files and copy information would not be exceeding the purpose authorization was given for, if authorization only related to a user code allowing plain access to information, it will instead be unauthorized use.

The important step towards adopting such an interpretation is the development of different levels of authorization codes, much like it has been done with documents that are secured from accessing, copying or modifying.

B. ENTITLEMENT FOR EXCEEDING AUTHORIZED ACCESS

Turning now to the topic of entitlement in order to assess how the notion of entitlement could be distinguished from authorization and could fill in the space *Nosal 2* created by eliminating the chance of having insiders "exceed authorization" in the sense of unintended use of authorization (the *Czubisnki* way). Reintroducing entitlement as distinct from "authorization in a technical sense" will also allow the introduction of unauthorized use by authorized access in different, yet potentially also punishable, or at least remediable, ways that are more appropriate to the goods being harmed and preserve the rationale in *Nosal 2* without, though, leaving blameworthy excesses unpunishable.

The following is an example to show how entitlement will be applied as a distinct term. An employee is authorized to access and copy information in terms of having personal passwords allowing him to go through technological restrictions, but he is not entitled to copy the information for personal purposes, according to explicit employer policies. No technical restriction exists to prevent the accessing employee from copying; thus, it is up to the employee's discretion to both access and copy, even though he should not copy the information. The concept of entitlement could help characterize these instances and distinguish them from unauthorized acts. In essence, entitlement can substitute for the current concept of exceeding authorized access in those cases where private contracts or agreements prohibit certain uses, while they have been made technologically feasible for insiders. Violating the limits of entitlement in terms of making unintended use of the existing level of authorization would, thus, signal the cases when prosecutors might need to assess the potential liability of the insider for breach of confidence, theft of trade secrets, or any other applicable offenses. In these

cases of insiders lacking the entitlement to make certain use of accessible information, the aforementioned sentencing guideline relating to a position of trust could also apply.[190]

Consequently, for CFAA offenses, there is only one condition of authorization—unauthorized use, yet with varying levels of use being allowed and where the existence of authorization relates to the particular level of use made compared to the use allowed by the imposed technological limitations. The concept of "exceeding authorized access" becomes devoid of meaning, something which *Nosal 2* and cases like *Shurgard* and *Citrin* essentially support and is substituted by entitlement, which relates to offenses other than those contained in the CFAA.

The element of entitlement and the exceeding of it could allow one to find legal solutions against contractually prohibited uses of information based on other offenses or civil law, since there would be no support for computer misuse offenses in these cases as no technological controls would be bypassed. That way, prosecutions or resolutions more generally would be possible through the use of more accurate provisions regarding problematic uses of information, such as the law of confidence or protection of trade secrets.

Consequently, linking CFAA prosecutions solely to bypassing technological controls, in the same way that *Nosal 2* has done, is important in reinstating the original dimensions of the CFAA as an act meant to punish computer misuse, either on its own or as a precondition to other crimes such as fraud. Moreover, using the term "entitlement" to define the cases when another law should resolve a conflict of misuse of information accessed by, primarily, employees and secondarily, users browsing websites and using online services, is very useful. The distinction facilitated by the suggested terminological changes will satisfy the rationale that *Nosal 2* promoted; thus, disconnecting the prospect of CFAA liability from website terms and conditions or employee contracts and computer use policies. The distinction will also provide a more clear-cut criterion for deciding when to employ the CFAA in violations of private agreements and terms of use of information and when to opt for more appropriate laws, such as those relating to trade secret theft or the breach private law-based confidentiality agreements and employment contracts. This rationale is also consistent with the bill suggested by Rep. Zoe Lofgren and Sen. Ron Wyden in order to eliminate the term of exceeding authorized access and retain only the term access without authorization which will mean:

> (A) to obtain information on a protected computer; (B) that the accesser lacks authorization to obtain; and (C) by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that in-

190. *See* DOYLE, *supra* note 75.

formation.[191]

C. *NOSAL*, THE NEW APPROACH, AND THE INTENTIONAL COMPUTER DAMAGE PROVISION

Other questions arise from the change in the concept of authorization, such as whether *Nosal 2* also impacts the intentional computer damage provision and whether there is also a need to revamp its phrasing in order to clarify and harmonize it with the new approach suggested by Nosal 2 and the view adopted above in terms of fragmenting the levels of authorization. This example will demonstrate how the new approach to authorization can generally produce more efficient and harmonized results.

The computer damage provision punishes "whoever . . . (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[192] The initial question that will have to be answered here is whether the computer damage provision is related to the above discussion. Most of the cases mentioned discussed herein have been linked to other offenses relating to unauthorized access or exceeding authorized access, such as obtaining information from a protected computer (Section 1030(a)(2)) or computer fraud (Section 1030(a)(4)). However, since the provision includes the notion of causing damage "without authorization," if authorization is redefined, then perhaps another look should be given to this provision and the consequences reconsidering the notion of authorization.

Before getting into the discussion of why the provision only mentions "without authorization" even though it is meant to be applicable to insiders that can also cause damage by exceeding their authorization (compared to the provisions relating to reckless or negligent damage that only apply to outsiders), one would first have to consider whether the phrase "without authorization" only relates to the term of damage or to the transmission of a program, information, code, or command as well. The history of the provision could imply that authorization also relates to the initial act of transmission since in the past the provision had been construed as outlawing: "intentional access . . . without authorization, and by means of . . . such conduct . . . prevent[ing] authorized use of any such computer . . . and thereby causes loss to one or more others of a value aggregating $1,000 or more . . . ," the government was not required to show that the defendant intentionally prevented use nor that he intentionally caused damage "aggregating $1,000 or more."[193]

---

191. *See* Lofgren & Wyden, *supra* note 11.

192. 18 U.S.C. § 1030 (2010).

193. United States v. Morris, 928 F.2d 504, 504 (2d Cir. 1991).

The prosecutors manual, however, makes the issue more complicated by advising that:

> by contrast (to the other subsections of the (a)(5)), section 1030(a)(5)(A) requires proof only of the knowing transmission of data, a command, or software to intentionally damage a computer without authorization. The government does not need to prove "access." Since it is possible to damage a computer without "accessing" it, this element is easier to prove (except for the mental state requirement). For example, where an attacker floods an Internet connection with data during a denial of service attack, the damage is intentional even though the attacker never accessed the site.[194]

If the government does not need to prove access, then it does not need to prove lack of authorization either—only the mental state needs to be proven. This would mean that the phrase "without authorization" relates only to damage and not to the transmission causing the damage. However, such an interpretation of "access" as something more than transmission of information to a website or computer network is seriously challenged.

The important issue here is whether transmission of data to reach a computer in the form of a denial of service attack would or would not mean that the computer is accessed, as the manual describes.[195] This is the basic step in order to then go into a discussion of whether the term "without authorization" attaches to the transmission of data as well as the damage. If the transmission is not access, but a stage prior to access, then there is no point in discussing whether "without authorization" attaches to both transmission and damage or solely to the latter.

If the terms "without authorization" attaches to the transmission and not just to the damage, since the provision applies to insiders as well as outsiders, there would be an important conceptual gap here where the term exceeding authorized access, which relates to insiders, will be missing from the provision. Thus, an amendment of the CFAA based on *Nosal 2* will also have to address the issues arising from the role of exceeding authorization in computer damage offenses.

1. Is a Transmission of Information Access?

With regard to access, there have been different interpretations based either on transpositions of real space concepts to the virtual world or based on the exchange of communication data between com-

---

194. OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATTORNEYS, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES, 37 (2011) *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

195. *Id.*

puters.[196] For the first approach, the mere sending of information would not constitute access, since a further act of going beyond the access restrictions of a protected proprietary network or database might be required. Alternatively, according to the communication-based approach, since every attempt to send information is met with a response, from a password prompt webpage to a normal webpage for publicly accessible websites, any transmission of information would be considered access.[197] The concept of access becomes particularly blurry, for publicly accessible websites where interaction and exchange of information does not require any further authorization or intrusion in the network beyond the publicly accessible page.

Case law has also been quite torn on the issue of access.[198] For example, in an early Kansas Supreme Court case, *State v. Allen*, the court followed the real/virtual analogy to argue that Allen had not gained access to the Bell Company computers since, according to the established evidence, he had only reached the stage where he was prompted to enter a password.[199] The court rejected an overtly broad definition of access in the law and opted for a dictionary interpretation of access, which was far narrower, as "freedom or ability to make use thereof."[200] The court discussed that Allen had not been able to make any use of the Bell computer before entering any right passwords to gain entry, something which was not proven by the evidence.[201] Of course, for public websites, making use would be different than making use of proprietary, closed networks, as the former do not require any additional information input stage, in contrast to password-protected networks.

Furthermore, in a similar case, *State v. Riley*, the court followed the statutory broad interpretation of access and found that getting the password prompt page and trying to guess passwords amounted to access.[202] Although this might seem extreme, one should consider that in order to get the password prompt page it means that he has made an initial contact with a page that is restricted and that this is its initial response, i.e., to communicate the restriction of further access or allow it.

More recently, courts have increasingly favored a broader interpretation of access that is consistent with the communication-based approach. For example, the court in the case of *America Online v. National Health Care Discount, Inc.* has interpreted emailing a computer as access, even based on the dictionary definition employed in the case of

---

196. Kerr, *Cybercrime's Scope*, *supra* note 12, at 1620.
197. *Id.* at 1620-21.
198. *Id.* at 1621.
199. *See generally* State v. Allen, 917 P.2d 848 (Kan. 1996).
200. *Id.* at 853.
201. *Id.*
202. *See generally* State v. Riley, 846 P.2d 1365 (Wash. 1993) (*en banc*).

Allen.[203] As Kerr argues: "To the *NHCD* court, access is a physical world concept, not a virtual world concept: The question is not whether the sender of the communication gains a virtual entrance into the computer from the sender's standpoint, but whether the communication itself is transmitted through the computer."[204] That would definitely render the transmission of the computer damage provision currently equal to access.

This is supported by additional cases relating to transmissions of information to publicly accessible websites. The court in *Explorica* has considered the transmission of the Scraper and the automated reading and compiling of the publicly accessible information as acts of exceeding authorized access even though the employees were just accessing information that was publicly available on open websites. A similar rationale regarding access to publicly available information simply as viewing and compiling lists of it has been adopted also in the case of *Register.com, Inc. v. Verio, Inc*.[205]

The court in *Nosal* has also considered plain users violating terms and conditions of websites as in danger of being considered liable for exceeding authorized access. The view of the *Nosal* court would mean that it also perceives access not just as having insider access to a protected company or public sector computer network, but even as interacting with publicly available websites by sending information requests. If such uses can be considered liable for exceeding authorized access, according to the broad interpretation of the term, then one would have to accept that the mainstream interpretation of access includes the interaction with a public website. If interaction with a website is considered access, then of course sending information to a public website in order to slow it down, as with the denial of service attacks example found in the prosecutors manual, would also be considered access; thus, the advice provided seems to be lacking in clarity and to be out of date.

Moreover, if the provision of intentional computer damage is to apply to both outsiders and insiders, which it is, as the *Citrin* court highlights[206] and the prosecutors' manual affirms,[207] the term "without au-

---

203. *See generally* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000).

204. Kerr, *Cybercrime's Scope*, *supra* note 12, at 1628.

205. Register.com, Inc. v. Verio, 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000).

206. "Congress was concerned with both types of attack: attacks by virus and worm writers, on the one hand, which come mainly from the outside, and attacks by disgruntled programmers who decide to trash the employer's data system on the way out (or threaten to do so in order to extort payments), on the other." Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

207. This subsection 1030(a)(5)(i) applies equally to offenders who are authorized to use the victim computer system (an "insider"), to those not authorized to use it (an "outsider"), and to those who have never accessed the system at all. OFFICE OF LEGAL EDUCATION EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, *supra* note 194.

thorization" should relate to the transmission of the data that causes the damage and not to the damage itself, since something that is considered damaging in the context of the computer damage will always be considered unauthorized (or exceeding authorization). If the act of impairment, modification, or deletion/destruction of data that could be damaging, is in fact authorized, it would not be considered damaging, as it would be done under permission, potentially as part of normal network management duties. Therefore, we cannot have an "authorized" transmission of data causing damage, having established that the transmission is access as well, which would, however, cause "unauthorized" damage with intent. Either the transmission would have to be unauthorized as well, coming from an outsider, such as a virus, or it will have to be at least exceeding authorized access of an insider, since it will relate to an act that will be making unintended use of authorization an insider will have.

Even if "without authorization" is to relate only to damage, since the provision is applicable to insiders that have some sort of access as well, there should at least be an additional phrase after the term "damage without authorization." An example would be to add "or by exceeding authorization" in order to relate to those cases where someone intentionally transmits data and causes damage by exceeding authorization, such as employees installing a virus that deletes files on their work computers, or even plain users getting together to DDoS a publicly accessible website, as with anonymous virtual sit-in protests. Having only the term "without authorization" implies that the provision only refers to outsiders or that *Citrin*'s approach of the principle of agency must be applied eliminating authorization even for insiders and also the concept of exceeding authorization. However, this latter prospect is highly unlikely to be the dominant rationale for authorization as *Citrin* has been criticised by many cases[208] and superseded by *Nosal 2*.

From the above, it can be inferred that the current wording of the intentional computer damage offense is not only vague in the sense of not clarifying whether without authorization relates to the act of transmission as well as to damage, but even though it is meant to apply to insiders causing intentional damage, it does not include the terms "by exceeding authorization" in addition to "without authorization." Consequently, there seems to be a need for an amendment of the provision in order to deal with the concept of authorization either as being relevant to the act of transmission in addition to damage or just in damage in relation to insiders. This means that we will have to discuss how *Nosal 2* impacts this provision and then how the suggested interpretation of authorization and entitlement could shape the wording of a

208. *Id.*

more specific intentional computer damage provision relating with the same clarity both to insiders and outsiders.

D. NOSAL, THE NEW APPROACH AND THE NEW INTENTIONAL DAMAGE PROVISION

Going through this conceptual labyrinth of authorization, it is important to say that in the case of the computer damage provision, as it is written at the moment, *Nosal 2* does not help to reach logical conclusions. Consequently, the CFAA's wording will need to be amended in order to counter phenomena where no technical restrictions are bypassed, but the nature of the access is damaging to a computer system and thus prosecutable by the CFAA. In a sense, the detachment of the computer damage provision from unauthorized access is a move towards that direction, but it goes only halfway, mixing up conceptual understandings of access and authorization that apply to other provisions of the Act in different ways.

Consequently, a new provision needs to be created that will entail all the important elements discussed above. The definition of the new provision for intentional computer damage could be worded as: "the making of unauthorized use (including both unauthorized access and exceeding authorized access as discussed above) of data or computer resources in ways that cause damage to the same or other data or computer resources."

Here we need to remind ourselves of the definition of damage: "any impairment to the integrity or availability of data, a program, a system, or information."[209] The question arising is whether someone might be authorized to cause such impairments for work purposes, but might be deleting information in order to prevent the employer from using it, while the employee plans to start a competing business. This action would fall within the scope of entitlement discussed above, where one modifies information by deleting it, but without violating any technical restriction as *Nosal 2* desires. Therefore, this action would not relate to intentional computer damage but to potentially civil violations. The installation of a virus on the same network in order to delete these files would however be unauthorized as it would be an act against the antivirus software/firewalls of the employer that will in most cases exist. Even if there is no bypassing of technical restrictions in the sense of gaining access to a network, there is unauthorized use in the sense of trying to bypass the antivirus technical safeguards.

Perhaps the most challenging issue here is the case of a denial of service attack on a publicly accessible website, done through the very mainstream, legitimate authorized use of repeatedly requesting infor-

---

209. 18 U.S.C. § 1030(e)(8).

mation from the website. In the cases where botnets are employed in addition, the charges for unauthorized use of data in order to cause damage will be based on the employing of computers that have been turned into zombie computers unintentionally by a hacker through the unauthorized transmission and use of a trojan-horse software. Therefore, the use of the zombie computers would be an act in violation of antivirus controls through the unauthorized installation of that software on computers protected by even meager technical restrictions. Under the suggested definition of intentional damage, botnet attacks would be unauthorized use of data or computer resources or programs that cause damage to other computers. The further consequence of such an interpretation is that activist protesters that are merely employing their personal computers to join in with others doing the same reloading and using only their own resources in order to protest by realizing a virtual sit-in would not be prosecutable by the intentional computer damage provision in general. Moreover, they will not be prosecutable under the reckless or negligent provisions since these offenses are meant for outsiders not having authorization to access to the website and, as has been established, for publicly accessible websites, access is authorized for everyone able to access the Internet.

In cases these protests are facilitated by botnets, prosecutors should make efforts to prosecute, not plain users, as has happened often, but those employing the botnets making unauthorized use of computer resources to cause damage. If plain users knowingly join in with groups that employ botnets then they could also be charged with conspiracy. However, plain users accessing a website and reloading it should not be considered felonious criminals that damage websites, as they would not be perpetrating any unauthorized action. Consequently, the interpretation of unauthorized use given here manages to allow prosecutions of dangerous denial of service perpetrators through armies of zombie computers, while allowing plain users to protest without serious legal consequences. As for those worrying that plain protesters might cause serious impairments, it has been argued that most websites today, especially governmental or corporate ones will have the infrastructure and defense mechanisms to absorb the amount of traffic generated by a few thousand protesters, if their efforts are not magnified by botnets.[210]

VI. CONCLUSION

As this Article has discussed, the concept of authorization is creating more problems and controversy than solutions for computer crime.

---

210. Jeff Bliss & Justin Blum, *Holder Says U.S. Probes Wikileaks-Related Web Attacks*, BLOOMBERG (Dec. 09, 2010), http://www.bloomberg.com/news/2010-12-09/holder-says-u-s-is-looking-into-wikileaks-tied-cyber-attacks.html.

It seems that it is high time for a radical change that will reinvigorate the CFAA and will modernize it in order to be able to constitute an efficient tool for dealing with serious cyber-criminality. Additionally, the CFAA should be amended to avoid being so vague as to allow for contested interpretations and excessive prosecutorial discretion, promoting instead a more harmonized application of its provisions. This Article aimed to highlight some of the most serious problems, conceptually and practically, and to suggest an alternative wording and conception for authorization that would be consistent with the above aims of harmonization, modernization, consistency of goals, and fairness of prosecutions. The recent developments in courts potentially indicate a more general shift towards a different approach to cybercrime, also backed by legislative proposals. It appears that we will soon be seeing some measure of reform.

In fact, in the EU, a *Nosal*-like approach is already being promoted with the new Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.[211] The new Directive establishes in Article 3 (Illegal access to information systems) that member States shall take the necessary measures to ensure that "[intentional unauthorized access][. . .] is punishable[. . .] where committed by infringing a security measure, at least for cases which are not minor."[212] Moreover, in Recital 17 it is clarified that:

> [C]ontractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability, where the access under such circumstances would be deemed unauthorised and would constitute the sole basis for criminal proceedings.[213]

Although implementation of this Directive is not due until 2015 and Article 1 explains that the Directive establishes minimum rules, allowing for deviations, it is, nonetheless, an additional indication that global perceptions regarding unauthorized access and exceeding authorized access might be changing towards a *Nosal*-like approach.[214] This can be especially so, since there are tools to deal with unauthorized uses of accessible information by insiders, such as data protection laws in the EU regarding personal data,[215] the common law tort of breach of confidence, or as in the case of *Nosal*, charges under economic espionage and theft

---

211. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA, 2013 O.J. (L 218).

212. *Id.* at art. 3.

213. *Id*. at Recital 17.

214. *Id.*

215. *See* UK Data Protection Act, § 55 (1998).

of trade secrets, such as those found in the Economic Espionage Act.[216] We can only hope that any changes will be of essence and not just a re-shuffling of the same notions and provisions. The signs seem to suggest we should be optimistic about seeing actual changes.

216. 18 U.S.C. § 1831 (2013); 18 U.S.C. § 1832 (2012).