Golden Gate University Law Review

Volume 43
Issue 1 *Ninth Circuit Survey*

Article 10

February 2013

United States v. Nosal: Separating Violations of Employers' Computer-Use Policies from Criminal Computer Hacking Invasions

Colette Thomason
Golden Gate University School of Law

Recommended Citation

Colette Thomason, *United States v. Nosal: Separating Violations of Employers' Computer-Use Policies from Criminal Computer Hacking Invasions*, 43 Golden Gate U. L. Rev. 163 (2013).
http://digitalcommons.law.ggu.edu/ggulrev/vol43/iss1/10

CASE SUMMARY

UNITED STATES v. NOSAL: SEPARATING VIOLATIONS OF EMPLOYERS' COMPUTER-USE POLICIES FROM CRIMINAL COMPUTER HACKING INVASIONS

*COLETTE THOMASON**

INTRODUCTION

Computer crimes are a worldwide threat.[1] Any individual with access to a computer may become victim to a computer crime. In the summer of 2010, the Pentagon alone received over six million hacking and security threats per day, or 250,000 an hour.[2] One of many measures to prevent computer crimes is the Computer Fraud and Abuse Act (CFAA), a federal statute that prohibits the unauthorized access of a

[*] J.D. Candidate, May 2013, Golden Gate University School of Law, San Francisco, California; B.A., Business Administration, 2005, University of Hawaii at Hilo.

[1] *See University Professor Helps FBI Crack $70 Million Cybercrime Ring*, ROCK CENTER WITH BRIAN WILLIAMS, (Mar. 21, 2012, 12:14 PM), www.rockcenter.nbcnews.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring (reporting that hackers from Eastern Europe allegedly stole $70 million from the payroll accounts of approximately 400 companies in America); *see also* Press Release, Fed. Bureau of Investigation, Six Hackers in the United States and Abroad Charged for Crimes Affecting over One Million Victims, (Mar. 6, 2012), www.fbi.gov/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims (reporting that hackers were charged with theft of confidential information from approximately 860,000 subscribers of Stratfor, a private geopolitical analysis firm, and that hackers had claimed responsibility for halting service to websites for Visa, MasterCard, and Paypal in early 2011, in retaliation for the payment companies refusing to accept donations to Wikileaks).

[2] *Governments Battle To Stay Ahead of Threats on Internet, "The Great Leveler,"* PBS NEWSHOUR (Aug. 10, 2010), www.pbs.org/newshour/bb/science/july-dec10/cybersec_08-10.html.

computer or computer data, such as when a hacker obtains bank account information from a financial institution's network.[3] There is currently disagreement among appellate courts as to the scope and application of the CFAA.[4] Some circuits apply the CFAA only to hacking crimes, while others include violations of a webpage's terms of service or an employer's computer-use policy.[5]

A violation of an employer's computer-use policy could be as minor as checking a personal Facebook page or personal bank account while at work. On the other hand, the violation of an employer's computer-use policy could be more egregious, as in the case of *United States v. Nosal*.[6] In *Nosal*, an en banc panel of the Ninth Circuit examined the scope of the CFAA as applied to an employee who used a work computer for personal purposes, addressing the issue of whether a violation of an employer's computer-use policy can be considered criminal hacking.[7]

I. BACKGROUND

The CFAA was enacted by Congress in 1984[8] and provides both criminal and civil penalties for unauthorized access to a computer.[9] The CFAA prohibits intentional and unauthorized access to a computer that results in the accesser obtaining information from any protected computer.[10] Under the CFAA, "protected computers" include those used exclusively for the use of financial institutions or the federal government, as well as those used in or affecting interstate or foreign commerce or communication.[11]

[3] 18 U.S.C.A. § 1030 (Westlaw 2012).

[4] Peter A. Crusco, *The "'Privatization' of Criminal Prosecution and the CFAA*," LAW TECHNOLOGY NEWS (June 20, 2012), www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1339937415222.

[5] *Id.*

[6] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

[7] *Id.* at 856 (stating that hacking is "the circumvention of technological access barriers"). Because of its size, the Ninth Circuit ordinarily uses a limited en banc court, consisting of the Chief Judge of the circuit plus ten additional judges drawn by lot from the pool of active judges. Rarely, a case heard by a limited en banc court may be reheard by the full court. *See* 9th Cir. R. 35-3; *see also* 28 U.S.C.A. § 46(c) (Westlaw 2012); Pub. L. No. 95-486, § 6, 92 Stat. 1629 (1978) (authorizing limited en banc courts for courts of appeals having more than fifteen active judges). *Nosal* was decided by a limited en banc court. *See Nosal*, 676 F.3d at 855.

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

[9] 18 U.S.C.A. § 1030 (Westlaw 2012).

[10] *Id.* § 1030(a)(2)(A)-(C). Besides information received from "any protected computer," the CFAA also prohibits obtaining information in a financial record of a financial institution, information on a consumer in a consumer reporting agency's file, and information from any department or agency of the federal government. *Id.* For simplicity, this Case Summary focuses on the prohibition relating to obtaining information from "any protected computer."

[11] *Id.* § 1030(e)(2).

The purpose of the CFAA is to prevent increasingly prevalent computer hacks.[12] The CFAA punishes whoever "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."[13] Therefore, the CFAA may be violated in two ways: either by accessing a computer without any authorization, or by having authorization for limited access and exceeding that authorized access.[14] The phrase "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[15]

The CFAA has been used by prosecutors in a variety of cases relating to the unauthorized use of computer data.[16] Unauthorized use commonly involves accessing a competitor's or former employer's database to obtain trade secrets, in order to cause damage to the competitor or former employer.[17] *Nosal* involved a former employee who obtained his former employer's confidential customer information from former colleagues still employed with the company.[18] Other cases have involved charges under the CFAA pertaining to violations of websites' terms of service agreements.[19]

A CFAA violation was alleged in a well-known federal criminal case involving the suicide of a teenage girl who was harassed on a social networking site by a classmate's mother.[20] Lori Drew was charged with violating the CFAA after allegedly "cyberbullying" thirteen-year-old Megan Meier, her teenage daughter's former friend.[21] Drew created a

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

[13] 18 U.S.C.A. § 1030(a)(4).

[14] *Id.* § 1030(a)(4); *see Nosal*, 676 F.3d at 864 (Silverman, J., dissenting).

[15] 18 U.S.C.A. § 1030(e)(6).

[16] *See* JONATHAN D. AVILA ET AL., PRIVACY COMPLIANCE AND LITIGATION IN CALIFORNIA § 4.21 (2008).

[17] *See id.*

[18] *Nosal*, 676 F.3d at 856.

[19] *See supra* note 16.

[20] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009). Not all allegations in the indictment were established at trial.

[21] *Id.* at 452. Lori Drew was charged with violating the portion of the CFAA that prohibits "accessing a computer without authorization or in excess of authorization and obtaining information from a protected computer where the conduct involves an interstate or foreign communication and the offense is committed in furtherance of a crime or tortious act." *Id.* (citing 18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(ii)). For example, Lori Drew used a photograph of a boy as the fictitious account's profile photo without the boy's consent, in violation of MySpace's terms of service. *See id.* at 452.

fictitious profile on the website www.MySpace.com ("MySpace"),[22] posing as a sixteen-year-old boy, and used the page to contact Meier.[23] The prosecution described the contact as "flirtatious."[24] After approximately a month of flirtatious contact, the fictitious "boy" reportedly sent Meier a message that he no longer liked her and that "the world would be a better place without her in it."[25] Megan Meier committed suicide that same day.[26] A jury convicted Lori Drew of a misdemeanor violation of the CFAA because she intentionally breached MySpace's terms of service.[27] The jury's guilty verdict was subsequently vacated by the federal district court.[28] The district court found that the conviction violated the void-for-vagueness doctrine because users of MySpace were not on notice that a breach of the website's terms of service could be a crime.[29]

A CFAA violation can also be alleged as a civil cause of action.[30] For example, an employer initiated litigation against a former employee who installed damaging software on a company computer.[31] The employee decided to leave the company and start his own competing business and installed the software before returning the computer back to the company.[32] The software destroyed data on the employer's computer

[22] *Id.* at 453. In *Drew*, a vice president of MySpace described MySpace as "a 'social networking' website where members can create 'profiles' and interact with other members." *Id.* MySpace accounts are free of charge, but members must be of a certain age, must provide personal information, such as their name and email address, and must agree to MySpace's terms of service and privacy policy. *Id.* It is not required that an individual read or even access the terms of service and privacy policy; all that is needed is a click on the "check box" stating that the individual agrees to the terms of service and privacy policy. *Id.*

[23] *Id.* at 452.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.* at 451.

[28] *Id.*

[29] *See id.* at 463 (explaining that "the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement") (quoting Kolender v. Lawson, 461 U.S. 352, 357-58 (1983)). As for the breach of a website's terms of service, the CFAA does not explicitly treat such a breach as a criminal act, and, as such, there were no clear guidelines for legal enforcement. *See id.* at 466-67. In the absence of clear guidelines as to when the intentional violation of a website's terms of service could lead to criminal penalties, the CFAA would be overbroad. *Id.* An extremely high number of Internet users could be turned into criminals, including not only those who create false MySpace accounts, but those who, for example, lie about their appearance or advertise the sale of girl scout cookies on MySpace. *See id.* at 466.

[30] 18 U.S.C.A. § 1030(g) (Westlaw 2012).

[31] Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[32] *Id.* at 419.

and permanently erased company information.[33] The Seventh Circuit held that the installation could violate the CFAA, and remanded the case for a determination by the trial court.[34]

In a similar instance, the First Circuit heard a case that involved a tour company that sued a competitor, alleging a CFAA violation.[35] Several employees of the competitor were former employees of the tour company.[36] The competitor used a software program that could access the tour company's prices from the company's website.[37] The defendant competitor created the software program based on its employees' knowledge of the tour company's proprietary codes.[38] The competitor then used the pricing information to undercut the tour company's prices.[39] The court of appeals affirmed the lower court's grant of an injunction, based on the CFAA, that barred the competitor from using the software program.[40]

A. FACTS OF *UNITED STATES V. NOSAL*

Defendant David Nosal was a former employee of Korn/Ferry International, a firm that provided services from executive recruitment to talent consulting and leadership development.[41] After Nosal left the company, he contacted several former coworkers who were still employed at Korn/Ferry and persuaded them to release confidential information to him.[42] Nosal planned to use the information to create his own competing business.[43] The information he obtained from his former co-workers included source lists, names and contact information for Korn/Ferry clients.[44]

Korn/Ferry's computer-use policy authorized employees to access such information, but employees were not authorized to release

[33] *Id.*

[34] *Id.* at 420. Since the appeal stemmed from the dismissal of the employer's suit, the court of appeals was not in a position to affirm a finding of a CFAA violation, but instead reinstated the case. *Id.*

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

[36] *Id.* at 579.

[37] *Id.*

[38] *Id.* at 580.

[39] *Id.* at 579.

[40] *Id.* at 585.

[41] United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc); *see* About Us, KORN/FERRY INT'L, www.kornferry.com/AboutUs (last visited Sept. 24, 2012).

[42] *Nosal*, 676 F.3d at 856.

[43] *Id.*

[44] *Id.*

confidential information outside of the firm.[45] Nosal was subsequently charged by the government, in part for aiding and abetting his former co-workers in "exceed[ing their] authorized access" in violation of the CFAA.[46]

B. PROCEDURAL HISTORY OF *UNITED STATES V. NOSAL*

The government charged David Nosal with numerous counts of trade secret theft, mail fraud, conspiracy, and criminal CFAA violations for computer invasion.[47] Several of the CFAA violations were related to aiding and abetting Korn/Ferry employees.[48] Nosal filed a motion to dismiss the CFAA indictments on the theory that misuse of information by employees with authorized access to the information was not proscribed by the CFAA.[49] Nosal argued that the CFAA was instead meant to prevent hackers from illegally accessing information, and did not apply to employees who misappropriate information.[50]

The district court denied Nosal's motion to dismiss the CFAA counts.[51] According to the district court, the Korn/Ferry employees used the information for a fraudulent purpose, which was equivalent to unauthorized access of information in violation of the CFAA.[52] At the point an employee has the "intent to defraud," the employee is no longer authorized to access corporate information.[53] Therefore, the court reasoned, the employee accesses the information "without authorization" or "exceeds [his or her] authorized access."[54]

Shortly after the district court's rejection of Nosal's motion to dismiss the CFAA counts, the Ninth Circuit decided a similar case that dealt with the CFAA.[55] The case was *LVRC Holdings LLC v. Brekka*, wherein the Ninth Circuit narrowly construed the CFAA's phrases "without authorization" and "exceeds authorized access."[56] The

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009); *Nosal*, 676 F.3d at 856.

outcome of *Brekka* caused Nosal to file a motion for reconsideration and a second motion to dismiss.[57]

The district court followed the analysis in *Brekka* and dismissed most of the CFAA charges "for failure to state an offense."[58] The government appealed the dismissal of these CFAA charges.[59] The Court of Appeals originally reversed and remanded the district court's decision,[60] but later granted rehearing en banc.[61] This Case Summary discusses the en banc decision.

II. THE NINTH CIRCUIT'S ANALYSIS

A. APPLICATION OF THE CFAA'S TERMS "WITHOUT AUTHORIZATION" AND "EXCEEDS AUTHORIZED ACCESS"

The Ninth Circuit explained that the CFAA was enacted to address the issue of computer hacking.[62] The phrase in the CFAA "without authorization" expressly prohibits access to an unauthorized computer.[63] The phrase "exceeds authorized access" is commonly applicable in the employment context when an employee has access to a corporate computer system but ventures outside the scope of his or her authorized access.[64]

The government agreed that the phrase "without authorization" prohibits hackers or outsiders from unauthorized access to computers.[65] However, the government disagreed with the district court's interpretation of "exceeds authorized access."[66] The government argued that the CFAA's phrase "exceeds authorized access" applies to persons who are authorized to use a certain computer, but who exceed that

[57] *Nosal*, 676 F.3d at 856.

[58] *Id.* (referring to the district court's opinion that "[t]here is simply no way to read [the definition of 'exceeds authorized access'] to incorporate corporate policies governing use of information unless the word alter is interpreted to mean misappropriate") (quoting United States v. Nosal, No. C 08-0237 MHP, 2010 WL 934257, at *7 (N.D. Cal. Jan. 6, 2010)).

[59] *Nosal*, 676 F.3d at 856 (noting that the district court dismissed five CFAA counts, which were the only counts before the appellate court).

[60] United States v. Nosal, 642 F.3d 781 (9th Cir. 2011).

[61] United States v. Nosal, 661 F.3d 1180 (9th Cir. 2011).

[62] *Nosal*, 676 F.3d at 856-57.

[63] *Id.*

[64] *Id.* at 856 ("The CFAA defines 'exceeds authorized access' as 'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.'" (quoting 18 U.S.C. § 1030(e)).

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

[66] *Id.* at 856-58.

authorized use.[67] In contrast, Nosal argued that "exceeds authorized access" does not apply to the use of the information in the computer, but strictly to access to that information.[68] According to Nosal's argument, an employee who has authorization to access a computer is not in violation of the CFAA simply because he or she misuses the information to which he or she had authorized access.[69]

The court rejected the government's argument on the basis of the language in the CFAA: "information . . . the accesser is not entitled so to obtain or alter."[70] According to the court, "entitled" is synonymous with "authorized."[71] The government argued that "entitled" means to be given a right, such that the Korn/Ferry employees exceeded their authorized access when they violated the rights given to them by the company's use policy.[72] The government further argued that the word "so" in this phrase is synonymous with "in that matter," which must refer to use restrictions.[73] The court rejected both arguments, declining to adopt the government's proposed broader interpretation.[74] The court explained that the word "so" is used as a conjunction and should not be given a substantive meaning without Congress's express intent to expand the scope of the CFAA by use of the word "so."[75]

According to the court, the government's proposed broad interpretation would result in the CFAA becoming "an expansive misappropriation statute" instead of the "anti-hacking statute" that it is.[76] The court thus favored Nosal's narrower interpretation of the CFAA—the phrase "without authorization" applies to outside hackers who have no authorized access to a computer, and "exceeds authorized access" applies to inside hackers who have authorized access but exceed the scope by accessing unauthorized files or data.[77]

[67] *Id.* at 856-57.

[68] *Id.*

[69] *Id.*

[70] *Id.* at 857 (referring to 18 U.S.C. § 1030 (e)(6), which provides that "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the *accesser is not entitled so to obtain or alter*." (emphasis added)).

[71] *Id.* at 857.

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.* at 857-58.

[76] *Id.* at 857.

[77] *Id.* at 858.

B. CFAA Interpretation Pursuant to the Rule of Lenity

In addressing the government's proposed meaning of the CFAA's language, the Ninth Circuit explained the concept of strict construction.[78] Strict construction is encompassed in the "rule of lenity,"[79] which requires that criminal laws be subject to a strict reading.[80] Therefore, when two possible readings of a criminal statute are plausible, it is necessary to select the narrower reading, unless Congress has unambiguously prescribed the harsher alternative.[81]

The rule of lenity helps guarantee that citizens will have notice of criminal laws and their accompanying penalties.[82] The Ninth Circuit emphasized that, should a broader interpretation of the CFAA apply, a large number of citizens would be subject to criminal penalties for the slightest violation of a terms of service agreement or corporate computer-use policy.[83] This could occur because it is not uncommon for an individual to exceed his or her authorized access to a computer.[84] For example, a member of a dating site may lie about their age when, as part of the dating site's policy, the member would have agreed to refrain from posting false information. If a strict interpretation of the CFAA were applied, the member could be charged with a CFAA violation.

If the court had accepted the government's proposed broad interpretation under the CFAA, employees who use company computers to check personal email, surf the Internet for personal reasons, or shop for personal goods could be subjected to criminal charges for a federal offense.[85] This could lead to FBI involvement and criminal penalties for even minor violations of corporate computer-use policies.[86] Such a broad interpretation would encompass a much larger spectrum of violations than Congress intended.[87] Consequently, the court determined the language of the CFAA was not meant to include mere violations of a corporation's computer-use policy.[88] Rather, the CFAA's purpose is to

[78] *Id.*

[79] *Id.*

[80] *Id.* at 863.

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.* at 860.

[86] *Id.*

[87] *Id.*

[88] *Id.*

prevent hackers from accessing computers that they have no authorization to access.[89]

The Ninth Circuit selected a narrower interpretation that prevents a flood of convictions and litigations for mere "unauthorized" use of computers,[90] holding that "exceeds authorized access" prohibits gaining unauthorized *access* to information, not the unauthorized *use* of that information.[91]

Moreover, criminal activities and the accompanying punishment must be clearly stated by Congress.[92] If, as is the case with the provision involved in *Nosal*, there is doubt concerning congressional intent, a court "must choose the interpretation least likely to impose penalties unintended by Congress."[93]

The Ninth Circuit's narrow interpretation of the CFAA's language "exceeds authorized access" prevented the government from having a successful argument.[94] The determination resulted from the Ninth Circuit's analysis of access restrictions versus use restrictions.[95] The "exceeds authorized access" language applies to access of information, not to use of information.[96] Therefore, the CFAA remains a prohibition that targets hackers who unlawfully gain access to computers, instead of a prohibition against misuse of information obtained through authorized access to a computer.[97] Consequently, the Korn/Ferry employees and Nosal were not subject to the CFAA's criminal sanctions.[98]

C. COMPUTER USERS SHOULD NOT FACE CRIMINAL LIABILITY FOR VIOLATING COMPUTER-USE POLICIES

The Ninth Circuit provided further support for a narrow interpretation of the CFAA by illustrating the potential consequences of a broader interpretation.[99] The court acknowledged that employees might frequently violate their employers' computer-use policies, whether by "g-chatting with friends, playing games, shopping or watching sports

[89] *Id.* at 858.
[90] *Id.* at 863.
[91] *Id.* at 864.
[92] *Id.*
[93] *Id.* at 863 (quoting United States v. Arzate-Nunez, 18 F.3d 730, 736 (9th Cir. 1994)).
[94] *Id.* at 864.
[95] *Id.* at 863-64.
[96] *Id.* at 864.
[97] *Id.*
[98] *Id.*
[99] *Id.* at 860-63.

highlights."[100] These violations, or "minor dalliances," could be considered federal crimes under a broad CFAA interpretation.[101] Employees who violate the CFAA under the government's broad interpretation could be threatened with criminal prosecution.[102] Employers may take advantage of this and enforce the CFAA at their whim, both subjectively and inconsistently.[103]

Further, the government's broad interpretation of the CFAA would result in uncertainty as to what constitutes criminal behavior.[104] Employees, who rarely read or understand their employers' computer-use policies, would not have sufficient notice of the criminal penalties they could be subject to for violating the use policies.[105] The court used the examples of not knowing whether using a company computer to check the weather for a business trip or to check on a company softball game would amount to a violation of the CFAA.[106] An employee may email a friend or relative instead of calling from the company phone.[107] Under the government's broad interpretation of the CFAA, the use of the computer, rather than the phone, would result in criminal liability.[108]

A broad interpretation of the CFAA would be problematic not only in the employment context, but also for the public's use of computers.[109] Internet use is often "governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands."[110] These private agreements are found on popular Internet sites such as Facebook, Amazon, IMDb, and YouTube.[111] The Ninth Circuit provided the example of Google's terms of service, which forbid use of Google's services by those who are not old enough to "form a binding contract with Google."[112] Another example provided by

[100] *Id.* at 860.

[101] *Id.*

[102] *Id.*

[103] *Id.* at 860 n.7 (noting that an employer is able to fire an employee for certain computer-use violations that are severe enough to justify termination, such as when an employee spends "six hours tending his FarmVille stable on his work computer"). Firing an employee is different from enforcing criminal penalties against the employee or having him or her arrested. *Id.*

[104] *Id.* at 860.

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.* at 860-61.

[110] *Id.* at 861.

[111] *Id.*

[112] *Id.* (citing Google's terms of service, effective Apr. 16, 2007-Mar. 1, 2012 § 2.3, www.google.com/intl/en/policies/terms/archive/20070416 ("You may not use the Services and may not accept the Terms if . . . you are not of legal age to form a binding contract with Google . . . .")).

the court is Facebook's terms of service that forbid allowing another person to log into a member's account.[113] Other examples are posting inaccurate information about oneself on eHarmony[114] and posting an eBay ad in the wrong category.[115]

According to the court, under the government's proposed broad interpretation of the CFAA, describing yourself on eHarmony as "'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit."[116] Not only are a website's terms of service often difficult to find and understand, but most websites reserve the right to revise their terms of service at any time.[117] It is unreasonable to believe Internet users will read a website's terms of service every time they access a particular website.[118] Internet users, in droves, could potentially be criminally liable for violations of various websites' terms of service if the government were allowed a broad interpretation of the CFAA.[119] Therefore, the court held, the CFAA's reference to "exceeds authorized access" does not apply to a violation of a company's computer-use policy.[120]

D. The Dissent: Knowledge and Intentional Fraud Should Be Weighed Heavily when Applying the CFAA

Judge Silverman wrote a dissent in which Judge Tallman joined.[121] The dissent focused on the facts specific to the case, the alleged "valuable proprietary information" that Nosal stole from Korn/Ferry, rather than "playing Sudoku, checking email, fibbing on dating sites, or any of the other activities that the majority rightly values."[122] Nosal's conviction stemmed from his, and his former colleagues', intentional

[113] *Id.* at 861 (citing Facebook Statement of Rights and Responsibilities § 4.8 www.facebook.com/legal/terms ("You will not share your password . . . [,] let anyone else access your account, or do anything else that might jeopardize the security of your account.")).

[114] *Id.* at 861 (citing eHarmony terms of service § 2(i), www.eharmony.com/about/terms ("You will not provide inaccurate, misleading or false information to eHarmony or to any other user.")).

[115] *Id.* at 861-62 (citing eBay user agreement, www.pages.ebay.com/help/policies/user-agreement.html ("While using eBay sites, services and tools, you will not: post content or items in an inappropriate category or areas on our sites and services . . . .")).

[116] *Id.* at 860.

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.* at 864.

[122] *Id.*

misuse of the company's confidential information and knowledge that such use violated the company's policy.[123] According to the dissent, the presence of fraud and knowledge set this case apart from the "far-fetched hypotheticals" offered by the majority.[124]

The dissent agreed with a recent Ninth Circuit case that interpreted "exceeds authorized access" as going beyond the limits of an individual's limited allowed use of a computer.[125] If an employee has access to a computer, but lacks access to certain files on the computer, then the employee would exceed his or her authorized access by accessing the restricted files.[126] As an example of this concept, the dissent explained that a consumer may test-drive a car a short distance, but driving the car to Mexico "on a drug run" would exceed the consumer's authority.[127] This interpretation allows the CFAA to cover both types of theft: the complete "unauthorized access" and the "exceed[ed] authorized access."[128]

The dissent's analysis falls in line with cases from the Third, Fifth and Eleventh Circuits which have held that the CFAA's phrase "exceeds authorized access" pertains to "employees who knowingly violate clear company computer restrictions agreements."[129] For example, the Fifth Circuit case involved an employee who violated her employer's computer-use policy by accessing confidential customer information in order to commit fraud.[130] The Eleventh Circuit held that a Social Security Administration employee who accessed personal information about former and potential girlfriends exceeded his authorized access.[131] Similarly, the Third Circuit upheld a CFAA conviction of a government contractor's employee who accessed confidential company information to obtain President Obama's student loan records.[132] The presence of knowledge and intentional fraud justified CFAA convictions in those cases.[133] In the dissenters' view, Nosal's knowledge and intent to defraud his employer by obtaining confidential information in violation of the employer's policy fell squarely within the phrase "exceeds

[123] *Id.*

[124] *Id.*

[125] *Id.* at 864-65 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)).

[126] *Id.* at 865.

[127] *Id.*

[128] *Id.*

[129] *Id.* at 865-66.

[130] *Id.* at 864 (citing United States v. John, 597 F.3d 263, 271-73 (5th Cir. 2010)).

[131] *Id.* at 864 (citing United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010)).

[132] *Id.* at 861 (citing United States v. Teague, 646 F.3d 1119, 1121-22 (8th Cir. 2011)).

[133] *Id.* at 866-67.

authorized access" in the CFAA.[134] Therefore, the dissent would have reversed the dismissal of the CFAA charges.[135]

CONCLUSION

In *Nosal*, the Ninth Circuit interpreted the CFAA strictly and narrowly, limiting the scope of the CFAA's phrase "exceeds authorized access."[136] In doing so, the Ninth Circuit ensured that employers would not be able to seek harsh criminal penalties for minor breaches of company computer-use policies.[137] At the same time, employers have other remedies available to enforce their computer policies, such as state criminal and civil actions. A broad interpretation of the CFAA could affect "millions of ordinary citizens," who might become subject to criminal punishment for a range of common activities.[138] Other circuits have chosen a broader interpretation of the CFAA that covers company computer-use policy violations or violations of a duty to loyalty.[139] In *Nosal*, the Ninth Circuit took the opportunity to urge the other circuits to reconsider their interpretation of "exceeds authorized access" in the CFAA.[140] The Ninth Circuit has laid a bright-line boundary as to what the CFAA does and does not cover.[141] In so doing, *Nosal* has created a split among the circuits that have considered the issue[142] and has invited speculation as to whether the Supreme Court will resolve the split.[143]

[134] *Id.*

[135] *Id.*

[136] 18 U.S.C.A. § 1030(e)(6) (Westlaw 2012).

[137] *Nosal*, 676 F.3d at 863-64.

[138] *Id.* at 862-63.

[139] *Id.* at 862.

[140] *Id.* at 863.

[141] *Id.* at 854.

[142] *Id.* at 863.

[143] *See* Richard Santalesa, *Ninth Circuit Narrows Reach of CFAA in En Banc US v. Nosal Decision*, INFO. LAW GRP. (Apr. 13, 2012), www.infolawgroup.com/2012/04/articles/computer-fraud-and-abuse-act-c/ninth-circuit-narrows-reach-of-cfaa-in-en-banc-us-v-nosal-decision.