Nos. 14-10037 & 14-10275

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAVID NOSAL,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of California, San Francisco
Case No. 3:08-cr-00237-EMC-1 (Hon. Edward M. Chen)

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT

Hanni Fakhoury
hanni@eff.org
Jamie Williams
jamie@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amicus Curiae
ELECTRONIC FRONTIER
FOUNDATION

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amicus Curiae* Electronic Frontier Foundation states that it does not have a parent corporation, and that no publicly held corporation owns 10 percent or more of the stock of amicus.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Other Authorities

STATEMENT OF AMICUS CURIAE[1]

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect digital rights. With roughly 23,000 dues-paying members, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF is particularly interested in the principled and fair application of computer crime laws generally and the Computer Fraud and Abuse Act ("CFAA") specifically. EFF has served as counsel or *amicus curiae* in key cases addressing the CFAA, including this case when it was previously before this Court. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (amicus); *see also United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (co-counsel); *United States v. Cioni*, 649 F.3d 276 (4th Cir. 2011) (amicus), *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus).

[1] No party's counsel authored this brief in whole or in part. No party or party's counsel contributed money that was intended to fund preparing or submitting the brief. No person—other than amicus curiae, its members, or its counsel—contributed money that was intended to fund preparing or submitting the brief. Neither party opposes the filing of this brief.

INTRODUCTION

The government's theory underlying this case—and approved by the district court—is that it is a federal crime to log into someone's online or electronic account with their credentials and with their permission. The result is that every husband who logs into his wife's Facebook account—with her knowledge and permission—has committed a federal crime. This Court, in this very case, has already rejected a broad interpretation of the Computer Fraud and Abuse Act ("CFAA") that would have resulted in "millions of unsuspecting individuals" finding out "they are engaging in criminal conduct." *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) ("*Nosal I*"). But the district court's decision to let the government pursue its theory of CFAA liability here, premised on the use of someone else's password with their permission, does precisely that.

The result is not simply a misinterpretation of *Nosal I* or an expansion of the CFAA beyond what Congress contemplated, but an unacceptably vague construction of a statute that creates different consequences for two nearly equivalent courses of conduct: it is now a crime for a person to use an authorized individual's password with their permission to access information for an improper purpose, but not a crime to ask that authorized individual to use their credentials to directly obtain the very same information themselves. This legal uncertainty means the possibility of capricious and discriminatory enforcement by the government.

This Court should reverse the decision below.

STATEMENT OF THE CASE

Nosal was an executive at Korn/Ferry executive search firm. *United States v. Nosal*, 930 F. Supp. 2d 1051, 1054 (N.D. Cal. 2013) ("*Nosal II*"). Korn/Ferry maintained a computer database with contact information for potential executive candidates. *Id*. In an effort to maintain the confidentiality of the information in the database, Korn/Ferry employees were issued unique usernames and passwords to access the database. *Id.* All employees were also required to sign agreements acknowledging that the information in the database could only be used for Korn/Ferry business. *Id.* at 1055. Any time an employee accessed the database, a pop-up banner warned: "[t]his computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution." *Id.*

Nosal decided to leave the firm to start his own company and, after he left Korn/Ferry, two current Korn/Ferry employees accessed information from the database on his behalf. *See id.* at 1055–56. It is undisputed that the employees had authority to access the database because they were still employed by Korn/Ferry at the time they obtained the information. One employee, J.F., also provided Nosal and other former Korn/Ferry employees with direct access to the database, either by logging into the system for them or by voluntarily providing them with her username and password. *Id.*

The government charged Nosal under 18 U.S.C. § 1030(a)(4), which makes it a crime to "knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access, and by means of such conduct further[] the intended fraud and obtain[] anything of value[.]" *See* 18 U.S.C. § 1030(a)(4). The government's theory was that Korn/Ferry employees had logged into the database to download information to give to Nosal at his request. Although the employees were all authorized to access the database, the government maintained they had exceeded their authorized access because they had violated the terms of Korn/Ferry's use restriction policy when they used that access for the purpose of giving data to Nosal rather than for Korn/Ferry business. In *Nosal I*, this Court, en banc, rejected this theory, ruling that CFAA liability could not be based on a computer user violating the terms of a use restriction policy. 676 F.3d at 859. As discussed in more detail below, this Court instead found the CFAA was designed to criminalize "the circumvention of technological access barriers." *Id.* at 863.

While *Nosal I* disposed of five of the eight CFAA charges against Nosal, this Court allowed the government to pursue the three remaining CFAA counts, which were based on instances in which former Korn/Ferry employees directly accessed the database, either after being logged in by J.F. or by using J.F.'s username and password, with J.F's permission, while J.F. was a Korn/Ferry employee and thus an "authorized" user.

Nosal again moved to dismiss the indictment, alleging the same defect in the government's legal theory: that there was no circumvention of a technological access barrier. The district court denied Nosal's motion to dismiss, finding that the government was not required to show that Nosal circumvented a technological access barrier to establish that he accessed the database "without authorization." *Nosal II*, 930 F. Supp. 2d at 1060–61. The district court relied on *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009), a case decided before *Nosal I*, which held that "[t]he plain language of the [CFAA] . . . indicates that 'authorization' depends on actions taken by the employer." The district court also found that even if circumvention of a technological access barrier was an element of a § 1030(a)(4) violation, the use of an authorized user's password, even with their permission, constitutes such circumvention. *Nosal II*, 930 F. Supp. 2d at 1061.

After a jury found Nosal guilty of the CFAA charges, he moved for an acquittal or new trial, again arguing that *Nosal I* ruled that there is no CFAA violation where the access in question was gained with the permission of the password holder and where there was no circumvention of any technological access barrier. The district court denied Nosal's motions, reaffirming its prior decision. *United States v. Nosal*, 2013 WL 4504652, at *3 (N.D. Cal. Aug. 15, 2013) ("*Nosal III*").

ARGUMENT

The district court erred by interpreting the CFAA to apply to behavior not rising to the level of circumventing a technological access barrier. While password protection is a technological access barrier, logging into someone's account with their full knowledge and permission—although perhaps a terms of service violation—is not a criminal circumvention of that technological access barrier. Imposing criminal liability for this act not only ignores this Court's prior decision in *Nosal I* and the legislative history and purpose of the CFAA, but it also makes criminals out of millions of ordinary Americans for innocuous behavior.

The CFAA convictions should be reversed.

I. COMPUTER FRAUD AND ABUSE ACT LIABILITY REQUIRES THAT THE GOVERNMENT PROVE THE CIRCUMVENTION OF A TECHNOLOGICAL ACCESS BARRIER.

Section 1030(a)(4) of the CFAA prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value[.]" 18 U.S.C. § 1030(a)(4). The question before this Court is whether the act of using the login credentials of an authorized user, with their permission, constitutes unauthorized access for purposes of the CFAA. Considering the clear purpose of the CFAA—to target computer trespassers who improperly obtain data that they do not have permission to obtain—this Court must find that it does not.

A. The CFAA Was Designed To Target "Hackers."

As this Court has repeatedly recognized, Congress' purpose when enacting the CFAA was to target "hackers" who "'intentionally trespass[ed] into someone else's computer files'" and obtained information, including information on "'how to break into that computer system.'" *Nosal I*, 676 F.3d at 858 (quoting S. Rep. No. 99-432, at 9 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2487). As this Court explained in *Brekka*, the CFAA "was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives[.]'" 581 F.3d at 1130–31 (quoting H.R. Rep. 98–894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)). Congress was addressing a narrow problem, not creating "a sweeping Internet-policing mandate." *Nosal I*, 676 F.3d at 858.

Relying on this legislative history, this Court has twice narrowed broad interpretations of the CFAA to maintain its focus as the federal anti-hacking statute.

First, in *Brekka*, this Court noted, "[n]othing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer." 581 F.3d at 1135. There, an employer sued a former employee under the CFAA for emailing documents from his work computer to himself in connection with establishing a competing business. *Id.* at 1129–30. This Court found no CFAA liability, holding that whether an employee using an employer's computer is acting with "authorization" depends not on the user's intent. Rather, the Court said "authorization" depends on the employer's explicit actions to grant or deny permission to use the computer or relevant content. *Id.* at 1135. The user's motivation for accessing the information did not render his access unauthorized under the CFAA. *Id.*

Then in *Nosal I*, this Court, en banc, reaffirmed its narrow construction of the phrase "exceeds authorized access" and rejected the argument that the bounds of an individual's "authorized access" turned on use restrictions imposed by an employer. 676 F.3d at 857. The Court held that the phrase "exceeds authorized access" within the meaning of the CFAA is limited to access restrictions, not use restrictions. *Id.* at 863. This interpretation was consistent with the "plain language of the CFAA" which "'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'" *Nosal I*, 676 F.3d at 863 (quoting *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (internal quotation marks omitted).

Other courts have reached the same result. Most recently, the Fourth Circuit—in an opinion issued after *Nosal I*—narrowly interpreted the CFAA because it was "unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy." *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012). Ultimately, *Brekka*, *Nosal I*, *WEC Carolina*, and other court decisions narrowly interpret the CFAA not only to consistently apply Congress's intent to criminalize "hacking," but also to avoid an unconstitutionally vague interpretation of the statute that would criminalize common, innocuous behavior.[2]

Nosal I instructs that CFAA prosecutions should be focused on "hacking—the circumvention of technological access barriers." *Nosal I*, 676 F.3d at 863. Neither Nosal nor his alleged accomplices circumvented any technological access barrier, and he therefore did not violate the CFAA.

B. The District Court Incorrectly Concluded That Circumvention Of A Technological Access Barrier Is Not Required.

The district court did not require that the government prove Nosal circumvented a technological access barrier. Rather, it ruled that *Nosal I* "did not . . . explicitly hold that the CFAA is limited to hacking crimes, or discuss the

[2] *See, e.g.*, *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013) (courts that have broadly interpreted the CFAA have "wrap[ped] the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use" and have "fail[ed] to consider the broad consequences of incorporating intent into the definition of 'authorization'"); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The plain language of the CFAA supports a narrow reading."); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929, 934 (W.D. Tenn. 2008) (the line of cases narrowly construing the CFAA "is the more correct interpretation"); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d at 967 (refusing to adopt an expansive definition of "authorization" for purposes of the CFAA, stating, "[t]he Court declines the invitation to open the doorway to federal court so expansively when this reach is not apparent from the plain language of the CFAA"); *Diamond Power Int'l., Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (identifying the narrower interpretation of "exceeding authorized access" as "the more reasoned view"); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005) (the CFAA is primarily a criminal statute "and, thus, should be construed narrowly").

implications of so limiting the statute" or "hold that the government is additionally required to allege that a defendant circumvented technological access barriers in bringing charges under § 1030(a)(4)." *Nosal II*, 930 F. Supp. 2d at 1060.

But while *Nosal I* did not explicitly say the government is required to prove a circumvention of a technological access barrier, that is the inescapable conclusion from both *Nosal I* and *Brekka* given this Court's repeated discussion of the CFAA as an anti-hacking statute.

The district court focused on *Brekka*'s discussion of "authorization" and this Court's belief that "it is the actions of the employer who maintains the computer system that determine whether or not a person is acting with authorization." *Nosal II*, 930 F. Supp. 2d at 1061 (citing *Brekka*, 581 F.3d at 1135). But that is simply another way of stating that circumvention of a technological access barrier is necessary for purposes of the CFAA.

Indeed, the way for an employer to indicate who is authorized and not authorized to access a computer system is to erect a technological access barrier to allow authorized users in and keep unwanted individuals out. Without some barrier to entry, everyone is "authorized" to access data. *See, e.g., Pulte Homes, Inc. v. Laborer's Int'l Union of N. Am.,* 648 F.3d 295, 304 (6th Cir.2011) (public presumptively authorized to access "unprotected website"); *Craigslist, Inc. v. 3taps, Inc.*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (making information on website publicly available gives everyone "authorization" to view it under the CFAA). In other words, the erection of a password barrier is what permits the employer to determine who has authorization to access a protected computer system or website.

In this way, this Court's holdings in *Brekka* and *Nosal I* are consistent with the idea that CFAA liability requires the circumvention of a technological access barrier, including one that may be set by an employer. The district court disregarded these important limitations and failed to maintain the CFAA's focus on "hacking" by failing to require the government to demonstrate the circumvention of a technological access barrier.[3]

C. Using The Login Credentials Of An Authorized User, With Their Permission, Is Not Circumventing A Technological Access Barrier Under The CFAA.

The district court also believed that even if circumvention of a technological access barrier was required, the government had made that showing because "password protection is one of the most obvious technological access barriers that a business could adopt." *Nosal II*, 930 F. Supp. 2d. at 1061. That is undoubtedly true but incomplete.

[3] That does not mean Korn/Ferry has no remedy for Nosal's act of accessing data from their proprietary database after he was no longer employed with the company. It is only to say that there is no CFAA liability on the facts here. As explained below, Nosal was also convicted of misappropriating trade secrets, a result *amicus* does not challenge.

If someone steals another's password or uses an authorized user's login credentials without their permission or knowledge, they have "circumvented" the password restriction, defeating a barrier to entry. *See The American Heritage Dictionary* (5th ed.), available at https://www.ahdictionary.com (last visited Dec. 8, 2014) (defining "circumvent" as: (1) "To surround (an enemy, for example); enclose or entrap"; (2) "To go around; bypass"; and (3) "To avoid or get around by artful maneuvering").

But that is not what happened here. Nosal did not access the database himself with his old and revoked employee credentials, nor did he steal someone else's credentials and access information without that person's knowledge and permission. Rather, Nosal allegedly conspired to use the login credentials of a former co-worker, still employed at Korn/Ferry and still authorized to access the Korn/Ferry database, with her knowledge and permission. Using an authorized user's credentials with that authorized user's permission does not result in someone circumventing, or avoiding, the technological access barrier because the person is effectively acting as the authorized user's agent or proxy.[4]

[4] In *Brekka*, this Court rejected the Seventh Circuit's reasoning in *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), that "authorization" for the purposes of the CFAA depends on the duty of loyalty agency principal. *Brekka* found that an employee's mental state cannot dictate the bounds of an employer's "authorization." *Brekka*, 581 F.3d at 1134. This Court reasoned that an interpretation of "authorization" granted by an employer or service provider based on a common law duty of loyalty created notice problems. *Id*. at 1135. But

An agent is someone who is "empowered to act for or represent another." *See The American Heritage Dictionary* (5th ed.), available at https://www.ahdictionary.com (last visited Dec. 8, 2014). Similarly, a proxy is someone who is "appointed or authorized to act for another." *Id.* As one prominent CFAA scholar has noted, "there are two parties that have plausible claims to set authorization: the owner/operator of the computer, and the legitimate computer account holder." Orin S. Kerr, Computer Crime Law 48 (3d ed. 2013).

This happens all the time in the online world, when a person gives a password to a spouse or friend to log into a password protected account and take some action on their behalf, such as sending an email, looking at their Facebook page, or checking an online bank account statement. For example, Charles Schwab's terms of service state "we ask you not to share your Registration information (including passwords, User Names, and screen names) with any other person for the purpose of facilitating their access and unauthorized use of Schwab

Brekka does not foreclose this Court from finding that an authorized individual may permit another individual to use her account as an agent or proxy. Indeed, the simple conclusion that a password holder may delegate another individual to access her account as their agent does not create the same notice problems that were a concern in *Brekka*. Moreover, the authorized user and the individual to whom she gives permission to access her account have no other superseding relationship. And in any event, when a criminal statute is susceptible to multiple interpretations, it should "be interpreted in favor of the defendants subjected to them." *See United States v. Santos*, 553 U.S. 507, 514 (2008).

Services."[5] But in the very next sentence, the same terms of service recognize that users will share their passwords with others, stating, "if you do share this information with anyone we'll consider their activities to have been authorized by you." In other words, the non-user is treated as the authorized user's agent or proxy.

There may be circumstances where an authorized user is prohibited from sharing their password with another individual or does not have the ability to delegate such control or agency because of a website's or computer's terms of use. Indeed, as the district court here noted, Korn/Ferry prohibited employees from sharing passwords. *See Nosal III*, 2013 WL 4504652, at *4. But basing liability on a violation of that company rule is simply repeating the problem that plagued this prosecution the last time it was before this Court: it imposes criminal liability on violations of office policy. *See Nosal I*, 676 F.3d at 863 ("the CFAA does not extend to violations of [a company's or website's computer] use restrictions"). The district court was wrong to conclude that using the login credentials of an authorized user with their permission circumvented a technological access barrier.

In reality, the district court was bothered that "what is being accessed by circumventing the password protection is Korn/Ferry's trade secrets," and thus

[5] *See*, *e.g.*, Charles Schwab, Terms of Use: Registration Information, Privacy, and Personalization, http://www.schwab.com/public/schwab/nn/legal_compliance/important_notices/terms.html (last visited Dec. 8, 2014).

believed CFAA liability was proper here. *See Nosal II*, 930 F. Supp. 2d at 1061 n.4. But this Court has already rejected this exact argument, noting the CFAA's "purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere," specifically in 18 U.S.C. § 1832. *See Nosal I*, 676 F.3d at 863. In fact, Nosal was separately charged and convicted of misappropriating trade secrets at trial. *See Nosal III*, 2013 WL 4504652, at *2, *13.

Because the Korn/Ferry database was accessed with the full knowledge and permission of an authorized user who used her credentials to log into the database, Nosal did not circumvent a technological access barrier.

II. THE DISTRICT COURT'S INTERPRETATION EXPANDS CFAA LIABILITY TO COMMON, INNOCUOUS BEHAVIOR.

This Court has already noted that the plain text of the CFAA is vague and open to varying interpretations. *Nosal I*, 676 F.3d at 856 (CFAA definition of "exceeds authorized access" "can be read either of two ways"); *Brekka*, 581 F.3d at 1135 (noting "the care with which we must interpret [the CFAA] to ensure that defendants are on notice as to which acts are criminal"). Vague laws invite "arbitrary and discriminatory enforcement" and "impermissibly delegate[] basic policy matters to policemen, judges, and juries for resolution on an *ad hoc* and subjective basis." *Grayned v. Rockford*, 408 U.S. 104, 108–09 (1972). When it comes to the CFAA, the statute's vagueness invites the risk that the government will "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Nosal I*, 676 F.3d at 860.

This Court must narrowly interpret the CFAA to avoid vagueness concerns. *See United States v. Skilling*, 561 U.S. 358, 402–03 (2010); *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). That means rejecting the government's argument that using someone else's login credentials with their knowledge and permission is a violation of the CFAA.

Just as in *Nosal I*, the government's proposed interpretation of "exceeds authorized access" expands the scope of the CFAA "far beyond computer hacking" and makes "criminals of large groups of people who would have little reason to suspect they [were] committing a federal crime." *See* 676 F.3d at 859. Specifically, it criminalizes nearly anyone who logs into someone's online or computer account with his or her permission.

For example, as noted by this Court in *Nosal I*, Facebook prohibits a user from sharing their username and password or from letting anyone else access their account. *See id.* at 861.[6] Under the government's interpretation of the CFAA, a

[6] Facebook's terms of service specifically state, "You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account." Facebook, Statement of Rights and Responsibilities 4.8, last revised Nov. 15, 2013, available at https://www.facebook.com/legal/terms (last visited Dec. 8, 2014).

husband who, with his wife's permission, logs into her account or accesses her profile has acted without authorization and is guilty of a federal crime.

While the specific CFAA section Nosal was charged with, § 1030(a)(4), requires an intent to defraud, the definition of the phrase "without authorization" in the CFAA "must apply equally to the rest of the statute pursuant to the 'standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning.'" *Nosal I*, 676 F.3d at 859 (quoting *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)). And in § 1030(a)(2)(C), the CFAA prohibits merely "intentionally access[ing] a computer *without authorization* or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer[.]" 18 U.S.C. § 1030(a)(2)(C) (emphasis added). In other words, the husband who logs into his wife's Facebook account with her permission has violated this provision of the CFAA. This is certainly not what Congress had in mind when it enacted the CFAA.

While the government may claim it would never prosecute such a trivial case, this Court has made clear people should not "have to live at the mercy of our local prosecutor." *Nosal I*, 676 F.3d at 862. As the Supreme Court has explained, the Constitution "protects against the Government; it does not leave us at the mercy of *noblesse oblige*" and courts should "not uphold an unconstitutional statute merely because the Government promised to use it responsibly." *United States v. Stevens*, 559 U.S. 460, 480 (2010). Interpretations of criminal statutes that "criminalize a broad range of day-to-day activity" should be rejected. *United States v. Kozminski,* 487 U.S. 931, 949 (1988).

The district court's interpretation of the CFAA also invites the precise sort of notice problems that render a criminal statute void for vagueness—situations where "ordinary people" cannot "understand what conduct is prohibited[.]" *Skilling*, 561 U.S. at 402. This Court has already ruled that Nosal could not be convicted of the CFAA for allegedly having former authorized coworkers log into a protected computer system to access or download specific information on his behalf. *Nosal I*, 676 F.3d at 864. But using the authorized coworker's credentials to access the same data directly (either via logging in on his own or having the authorized coworker log in and then turn the terminal over to him or one of his co-conspirators) is, according to the district court, a violation of the CFAA. *See Nosal II*, 930 F. Supp. 2d at 1061–63. These two situations illustrate almost equivalent courses of conduct. They both involve access to a database for an improper purpose. They both involve Nosal ultimately receiving data he was not entitled to access with his own expired credentials. And they both presumably involve the same harm: Korn/Ferry losing proprietary trade secrets.

The only distinction between the two scenarios is the means of access, a factor controlled exclusively by Korn/Ferry's prohibition on the sharing login credentials with others.[7] In other words, the same concerns that prompted this Court to reject a broad interpretation of the CFAA in *Nosal I*—that premising CFAA liability on use restriction policies would "allow[] private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law"—are present here. *Nosal I*, 676 F.3d at 860. The district court's decision thus presents a risk of legal uncertainty, rendering ordinary people unable to understand what conduct is prohibited. *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007).

The district court here looked only at the behavior of the defendant before it, failing to consider the effect of its decision on millions of ordinary citizens given the statute's unitary definition of "without authorization." *See Nosal I*, 676 F.3d at 862. In so doing, the court failed to apply the long-standing principle that courts must construe ambiguous criminal statutes narrowly so as to avoid "making criminal law in Congress's stead." *See Santos*, 553 U.S. at 514. Because the CFAA was never intended to apply so broadly, this Court should reverse the district court's decision and vacate Nosal's CFAA convictions.

[7] Naturally, the prohibition on sharing login credentials with others is motivated in part by the same reason why a Korn/Ferry employee is not permitted to access the database for non-work related purposes: it keeps valuable proprietary information under the control of Korn/Ferry.

CONCLUSION

The CFAA was "designed to target hackers[.]'" *Brekka*, 581 F.3d at 1130; *see also Nosal I*, 676 F.3d at 858. The district court's decision loses sight of this purpose and misinterprets both *Brekka* and *Nosal I* in a way that expands the CFAA to criminalize innocuous activities far beyond what Congress contemplated when writing the statute. This Court should reverse Nosal's CFAA convictions.

Dated: December 9, 2014

Respectfully submitted,

/s/ Hanni Fakhoury
Hanni Fakhoury
Jamie Williams
ELECTRONIC FRONTIER
FOUNDATION

Counsel for Amicus Curiae
ELECTRONIC FRONTIER
FOUNDATION

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae In Support Of Party-of-Interest-Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,829 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: December 9, 2014

Respectfully submitted,

/s/ Hanni Fakhoury
Hanni Fakhoury
Jamie Williams
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Counsel for Amicus Curiae
ELECTRONIC FRONTIER
FOUNDATION

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on December 9, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: December 9, 2014

/s/ Hanni Fakhoury
Hanni Fakhoury

Counsel for Amicus Curiae
ELECTRONIC FRONTIER
FOUNDATION