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* NOVELPOSTER IN SUPPORT OF THE UNITED STATES – APPELLEE

DAVID NIED
dnied@astralegal.com
KEENAN W. NG
kng@astralegal.com
MICHAEL S. DORSI
mdorsi@astralegal.com
AD ASTRA LAW GROUP, LLP
582 Market Street, Suite 1015
San Francisco, CA 94104
Telephone: (415) 795-3579
Facsimile: (415) 276-1976

Counsel for *Amicus Curiae*
NOVELPOSTER

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amicus Curiae* NovelPoster 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

Cases

Statutes

Other Authorities

STATEMENT OF THE *AMICUS CURIAE*[1]

NovelPoster is a San Francisco-based business that sought civil remedies available under the Computer Fraud and Abuse Act ("CFAA"). *See NovelPoster v. Javitch Canfield Group et al.*, No. 3:13-cv-05186-WHO, 2014 U.S. Dist. LEXIS 106804, 4–9 (N.D. Cal. Aug. 4, 2014). NovelPoster settled its case on February 3, 2015.

NovelPoster is representative of many businesses that have come to fruition because of the Internet and development of cloud-based computing. All of its business accounts are online and it primarily interacts with its consumers through the Internet. NovelPoster has an interest in ensuring that it and similarly situated businesses receive protections under the CFAA that Congress intended so that it and other entrepreneurs can continue to securely invest in and invent new businesses and technologies.

[1] Counsel to the parties have consented to the filing of this brief. 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.

INTRODUCTION

The Computer Fraud and Abuse Act provides valuable remedies for victims of invasions of digital privacy and data theft. The statute authorizes compensation for damage and loss, including impairment and unavailability of data, the cost of damage assessment, and data restoration expenses. It also authorizes injunctions. These remedies are often unavailable under common law or other statutes.

Defendant-appellant David Nosal asks this Court to impose a *technical access barrier* rule that would invalidate claims under the CFAA if the perpetrators were insiders or otherwise did not need to circumvent any technical access barrier. This is misguided. The proposed rule lacks any basis in the statute, would base liability on technical measures in the place of legal rules, and would impair the rights and remedies of computer fraud victims. This Court should reject the *technical access barrier* requirement.

Nosal also argues that use of another person's password, solely with the password holder's consent, should not qualify as a violation of the CFAA. This argument suffers from the same error as the technical access barrier argument: it presumes that because a person can easily perform the act, it is not wrongful. Not so. There are real victims who seek protection under the CFAA, and the civil and criminal remedies that Congress provides for them will be severely curtailed if this Court adopts Nosal's position.

STATEMENT OF THE CASE

For purposes of this brief, three facts are relevant: (1) Working at the behest of David Nosal ("Nosal"),[2] Becky Christian and Mark Jacobson used a password belonging to Jacqueline Froehlich-L'Heureaux to access Korn/Ferry's computer; (2) Korn/Ferry had revoked Nosal, Christian, and Jacobson's authorization, and explicitly prohibited Froehlich-L'Heureaux from sharing her password; and (3) for this wrongdoing, a federal jury convicted Nosal under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4) (2005).

ARGUMENT

In its first review of this case, this Court concluded that the CFAA does not restrict the *use* of a computer, only *access* to a computer. *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (*en banc*). Although the Court considered issues beyond the use/access distinction, including the purpose of the CFAA, technical access barriers and password sharing, the Court did not reach a conclusion or state a legal rule on those questions. These issues are now before this Court. This brief addresses two legal questions: (1) whether the CFAA requires the circumvention of a technical or code-based access barrier, and (2) whether an authorized user's sharing of a password, when that user is not authorized to share the password, renders access authorized. The answer to both questions is no.

[2] Nosal's liability for the actions of others is beyond the scope of this brief.

I. INTERPRETTING THE WORDS *WITHOUT AUTHORIZATION* TO REQUIRE CIRCUMVENTION OF A TECHNICAL ACCESS BARRIER LACKS A BASIS IN STATUTORY TEXT, PURPOSE, OR GOOD PUBLIC POLICY

A. A Technical Access Barrier Rule Would Contradict the Text and Purpose of the CFAA.

The CFAA imposes liability for actions taken *without authorization*. The statute does not state that acting *without authorization* is limited to actions that circumvent technological or code-based barriers to access. If Congress had intended to require such circumvention, it would have said so, as it has done in other statutes. *See, e.g.*, 17 U.S.C. § 1201 (2014) (making it a crime to "circumvent a technological measure that effectively controls access to a work protected under" copyright law).

Nosal's proposed interpretation of *without authorization* is also incompatible with the several provisions of the CFAA that criminalize activities that do not require accessing a protected computer. Subsection (a)(5)(A) makes it a crime to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A) (emphasis added),[3] *see also* 18 U.S.C. §1030(a)(6) & (7). The absence of an access requirement is incompatible with the proposed requirement that a defendant circumvent a technical access barrier.

[3] Additional requirements that applied at the time of Nosal's conduct have since been amended.

Subsection (a)(5)(A) protects the important rights of computer users from interference, whether the interference comes from persons who circumvent technical access barriers, or persons who do not need to. Even prominent advocates have applauded statutes, including subsection (a)(5)(A), for offering protection to persons with legitimate rights to access computers and data. *See, e.g.*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1660–61 (2003).

Nosal and EFF argue that the term *without authorization* should be interpreted to require circumvention of a technical access barrier, in part because (1) the absence of such a rule would compel an overly broad interpretation of subsection (a)(2)(C), and (2) the same interpretation must apply to subsection (a)(2)(C), the broadest provision, and subsection (a)(4), at issue here. *See* Brief of *Amicus Curiae* Electronic Frontier Foundation ("EFF Br."), p. 18 (Dkt. No. 14), *see also* Appellant's Opening Brief ("Appellant Br."), p. 27 (Dkt. No. 13-1).[4]

Nosal and EFF are correct concerning the uniformity of interpretation. Once a court defines a term for the purpose of one subsection, "that definition 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*, *supra*, 676 F.3d at 859 (quoting

[4] Docket numbers for this case are the docket numbers in Case No. 14-10037.

Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007)); *see also* Recent Case: United States v. Nosal, *676 F.3d 854 (9th Cir. 2012) (en banc)*, 126 Harv. L. Rev. 1454, 1456. Because this Court's interpretation of *without authorization* for purposes of subsection (a)(4) would apply not only to subsection (a)(2)(C), but also to subsection (a)(5)(A), this constraint is fatal to the interpretation proposed by Nosal and EFF.

In addition to imposing an access requirement that cannot be found in subsection (a)(5)(A), the technical access barrier rule would render legal a broad range of wrongful conduct, so long as the person engaged in behavior that did not circumvent a technical access barrier in order to access the computer.

The allegations pled in *NovelPoster v. Javitch Canfield Group, et al.* form a useful example of the pernicious results of applying a technical access barrier rule.[5] NovelPoster alleged that the three defendants had acquired the administrator credentials to NovelPoster's online accounts, including email and business accounts, as part of a business deal. The defendants then used those administrator credentials to change the passwords to email and other online accounts belonging to NovelPoster and its owners, locking the owners out of their own accounts and

[5] *NovelPoster* settled while cross-motions for summary judgment were under submission. *See* Dkt. Nos. 189 & 193, *NovelPoster v. Javitch Canfield Group, et. al.*, Case No. 3:13-cv-05186-WHO (N.D. Cal. dismissed upon settlement Feb. 4, 2015). Accordingly, all discussions in this brief refer only to matters as considered at the pleading stage.

allowing defendants to snoop through NovelPoster's archived email and other archived data. *See NovelPoster v. Javitch Canfield Group, et al.*, No. 3:13-cv-05168-WHO, 2014 U.S. Dist. LEXIS 106804, 5–8 (N.D. Cal. Aug. 4, 2014).

Two of the defendants moved to dismiss, asserting that their actions did not circumvent a technical access barrier. The court rejected this position, holding that, "to the extent that the defendants fault NovelPoster for not erecting a technological access barrier, it was the defendants' own alleged actions that prevented NovelPoster from doing so . . . the defendants kept NovelPoster from taking the precise action they now assert it failed to take." *Id.* at 23. The court was only able to engage in this analysis because it could reasonably conclude that the Ninth Circuit's ruling in *Nosal* did not require that defendants circumvent a *technical access barrier*. *See id.* (citing *United States v. Nosal*, 930 F. Supp. 2d 1051, 1060 (N.D. Cal. 2013)).

Alternatively, if CFAA liability did turn on technical access barriers, it could create a *race to the passwords* situation, where the first party to change the passwords would be immune from liability, and the other party, even if a rightful owner, would have no remedy under the CFAA. Making matters worse, under a technical access barrier rule, the CFAA would prohibit the victim from using its own technical methods to regain access to its own computers, because its own attempts to regain control could be circumventing a technical access barrier. Two state court cases, brought under state computer crime statues, demonstrate the particular danger of such situations when the conflict occurs between an employer and an employee tasked with designing or operating computer systems.

In *People v. Childs*, 220 Cal.App.4th 1079 (2013), California prosecutors brought charges against Terry Childs, a former network engineer for the City and County of San Francisco. A jury convicted Childs of violating California Penal Code § 502, the state law largely analogous to the CFAA. The jury concluded that Childs took control of the city's network infrastructure, and refused to provide anyone else with the username and password, effectively locking the city out of its own computer network. *See Childs*, *supra*, 220 Cal.App.4th at 1093. Childs challenged his conviction on appeal, alleging that he could not be convicted because he was authorized to access the system — a defense that would prevail under a technological access barrier rule. *See id.* at 1102. The California Court of Appeals rejected Childs' contention, finding that the state made an adequate showing that Childs did not have permission to lock city government out of its own systems.

The Court of Appeals of Georgia encountered a similar situation and reached the same result in *Fugarino v. State*, 531 S.E.2d 187 (Ga. Ct. App. 2000). Sam Fugarino was a computer programmer for a private company. After some workplace disputes, Fugarino deleted company some files on the company computer, and imposed password restrictions on other files, and refused to share the passwords. A jury convicted Fugarino for computer trespass, O.C.G.A. § 16-9-93(b).

Fugarino appealed, contesting that the state could not prove beyond a reasonable doubt that he knowingly acted "without authority." Fugarino, like Childs, was an insider and did not need to circumvent any technical access barriers in order to inflict damage. But the Georgia Court of Appeals did not impose a technical access barrier requirement. Rather, the court held that authority ran from the permissions granted by the owner of the computer network and affirmed Fugarino's conviction. *Fugarino*, *supra*, 531 S.E.2d at 189.

The situations that led to convictions in *Childs* and *Fugarino* are clearly covered by the plain meaning of the statute even though the defendants may not have circumvented technical access barriers.[6]

B. Good Public Policy Weighs Against a Technical Access Barrier Rule

[6] A technical access barrier rule might also render Denial of Service ("DoS") attacks outside the scope of the CFAA. "'A DoS attack occurs when the attacker floods the target website with e-mails and/or information requests, so that the website cannot respond to normal, legitimate user traffic. Legitimate users therefore experience a 'denial of service' because they cannot access the target website.'" *Massre v. Bibiyan*, No. 12-civ-6615 (KPF) 2014 U.S. Dist. LEXIS 82444, 2-3 fn. 2 (S.D.N.Y. June 16, 2014) (quoting Complaint), *see also eBay Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (considering DoS attack as potentially analogous to cookie stuffing). Under the plain meaning of the statute, a DoS attack would be a violation of subsection (a)(5)(A), causing damage by impairing the "availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8) (definition of damage). However, such an attack need not circumvent any technical or code-based barrier.

The valid concerns of current and potential victims of computer fraud counsel against requiring circumvention of a technical access barrier. First, such a rule would add a tangible, physical requirement to the authorization element. Setting up a technical access barrier, even something as simple as a password, necessarily requires the owner of the protected computer to take an additional step of action beyond simply expressing or denying authorization. Such a requirement would prejudice less sophisticated computers users who may be unaware of how to erect a technical access barrier, or those who do not have the resources to set up those hurdles.

Comparing the CFAA to the tort of trespass provides a useful analogy. A landowner can terminate access without having to physically remove a person in ordinary trespass situations. But under a technical access barrier requirement, it would not be enough for a landowner to announce, “Get off my lawn!” in order to show a claim for trespass. Rather, the landowner would be required to physically restrain the trespasser by putting up a fence or physically coercing the trespasser off of her property. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-1073 (9th Cir. 2004) (comparing the tort of trespass to the Stored Communications Act, 18 U.S.C. 2701, discussing meaning of “valid authorization”). The CFAA should not require the victim to put up additional, physical defenses beyond communicating authority, or lack thereof.

Second, a technical access barrier requirement severely narrows the scope of the authorization element. There are innumerable ways of communicating that someone is not authorized to access a protected computer without using a technical access barrier. Access revocation could be communicated orally, in writing or implied through conduct — such as with employment termination. *See, e.g.*, *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1136 (9th Cir. 2009) (this Court noting that both parties agreed that if defendant had accessed a company website after he left the firm defendant would have accessed a protected computer *without authorization*), *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (website demonstrated revocation of access by sending cease-and-desist letters to user)).

Under a requirement that a technical access barrier be circumvented, an employer providing written notification to an employee he is not authorized to access computer files — or even an employer firing the offending employee — would be insufficient to show that the employee is acting "without authorization."

Third, given rapidly changing technology standards, requiring a technological access barrier ensures the law will always struggle to define it and could require a complex understanding of technology to determine if the mechanism was a requisite barrier. This could make the understanding of "without authorization" a moving target based on the latest technological developments.

Understandings will be slowed further by the time it takes for courts to react. This case provides a useful example. When Nosal left Korn/Ferry in October 2005, smart phones, as we think of them today, were "unheard of . . . [but] a significant majority of American adults now own such phones." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). In October 2005, companies, Korn/Ferry included, tended to need centralized servers for their data. *See* Appellee Br., p. 7. Today, a host of new companies are able to scale rapidly due to reliance on cloud computing. Brief of Amicus Curiae BSA The Software Alliance, p. 7–13 (Dkt. No. 17). And while today Nosal expresses concern that the CFAA might criminalize a parent reading a child's Facebook account, in 2005 Facebook had just become available to high schools. *See* Appellant Br., p. 19. What might have been seen as a technical access barrier in 2005 may scarcely be recognized today. Yet Nosal and EFF would not only excuse liability based on technical access barriers, but also impose criminal liability based on a court's understanding of those barriers. In contrast, the concept of authority — as opposed to trespass — is one with a long history of legal analysis, and that courts are routinely able to grasp. *See, e.g.*, *Hickman v Maisey*, 1 Q.B. 752 (1900). It frequently requires no technical knowledge to understand and is part of the common human experience.

Fourth, requiring a circumvention of a technical access barrier excludes potential CFAA violations where the defendant prevents the victim from erecting technical access barriers. A technical access barrier rule could create a *race to the passwords*, whereby the first party control the system would gain an advantage of legal significance. Courts faced with these particular facts, and not bound by appellate courts dictating a technical access barrier rule, see the problem with such a construction. *See, e.g., Childs, supra*, 220 Cal.App.4th at 1101. This cannot be what the drafters of the CFAA intended.

II. USE OF A PASSWORD, AUTHORIZED BY THE PASSWORD HOLDER BUT PROHIBITED BY THE COMPUTER'S RIGHTS-HOLDER, IS A VIOLATION OF THE CFAA

This Court engaged in an illuminating discussion of the meaning of hacking during the previous en banc oral argument in this case. Ted Sampsell-Jones, representing Nosal engaged in the following colloquy with Judge McKeown, attempting to distinguish the charges now on appeal from the charges on appeal in 2011:

> Mr. Sampsell-Jones: I don't think that's quite the same as picking a lock or stealing.
>
> Judge McKeown: Well the one who's left, has a key that he or she didn't, quote, turn in, so to speak.
>
> Mr. Sampsell-Jones: No the one who's left doesn't have a key anymore. The one who has left gets the key consensually from the one who is still there.
>
> Judge McKeown: That's called hacking."

Oral Argument, *Nosal*, *supra*, 676 F.3d 854, at 46:45–47:10, *available at* http://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000006176.

Authorization under the CFAA derives from either (1) an underlying right of authorization, or (2) a grant of authorization by a person who has legal authority to grant authorization. *See Brekka*, *supra*, 581 F.3d at 1133. The CFAA protects the privacy rights and data of the computer system owner. Allowing an exception for password sharing by anyone else who happens to have a password would undercut the computer system owner's power to determine who can and who cannot access their computers.

Nosal and EFF's arguments on this subject break along two lines. First, they argue that this Court's prior decision applies only to hacking. This argument suffers from the same infirmities as the arguments concerning a technical access barrier. Second, Nosal and EFF marshal a parade of horribles, attempting to argue by analogy using cases that did not actually happen.

Regarding the latter argument, Nosal first analogizes Froehlich-L'Heureaux sharing of a password to the son of a homeowner sharing of keys to the house. Appellant Br., p. 22 (citing Cal. Penal Code § 602).[7] The U.S. District Court for the Northern District of California already interrogated a similar analogy. In *NetApp, Inc. v. Nimble Storage*, the court explained:

> NetApp analogize[d its] case to a conventional property crime, arguing that "[u]nder Reynolds' theory, a thief has license to burglarize a house

[7] Nosal's brief cites to § 620, but the quoted text is in § 602. Amicus NovelPoster assumes this is a typographical error and responds to what it understands to be the intended substance.

> because a window is left open." However, a closer analogy would be a situation where a houseguest receives a key, is then told he is no longer welcome but keeps the key, and the homeowner neglects to change the lock. Reynolds's arguments suggest that if the former houseguest continues to re-enter the house, the houseguest would not be acting "without authorization" or "exceed[ing] authorized access," even though he knows he may not return.

NetApp, Inc. v. Nimble Storage, No. 5:13-cv-05058-LHK, 2014 U.S. Dist. LEXIS 65818, 38 (N.D. Cal. May 12, 2014) (citation omitted). Judge Koh concluded that, of course, the CFAA applies. *See id*.

Nosal's proposed situation merits a more egregious analogy: the homeowner changes the locks and excludes the former houseguest, but the former houseguest contacts another person who possesses a key — perhaps a maid or dog walker — and continues to enter the house even after the owner tells the houseguest that he is no longer welcome. Of course this is a crime.

The maid and dog walker are useful to deconstruct the legal basis for the analogy. They might share a key with persons who the owner does not know exist, let alone intends to grant access. Such recipients of a key would be trespassers because the maid or dog walker, whether or not they were in some way agents of the owner, did not have authority to share access to the property. *Cf. McInerney v. City & County of San Francisco*, 466 Fed. Appx. 571, 573 (9th Cir. 2012) (concluding that the term *agent* in Cal. Penal Code § 602 has meaning in relation to specific authority).

Moreover, Nosal's argument is infinitely regressive. Under his interpretation, a person who knows a working password could share the password with someone, who could share the password with someone else, and on and on. It is unclear if the computer owner would have any legal recourse to stop the password sharing, creating the same problems as a technical access barrier rule.

Next, Nosal offers a set of examples of innocuous behavior that might violate the statute (assuming that no other limitations apply to section (a)(2)(C) — a question that is not before this Court). These examples include a husband sharing an email password with his wife, a parent logging on to her daughter's Facebook account, and a surviving spouse logging in to the decedent's bank accounts. Each of these examples can be changed to an egregious invasion of privacy by only slight changes in the facts. First, if a husband gives the password for his wife's email account to his mistress, she would then be able to actively plan how to avoid being discovered. The daughter, possibly forgetting that she once gave her mother her Facebook password, might find her mother snooping on her activities well into her mid – twenties. And if the decedent had a partner with the password but was not married to that partner, snooping in the accounts might provide the unmarried partner an opportunity to engage in fraudulent transfers to the detriment of the decedent's heirs.

Nosal asks this Court to limit the scope of subsection (a)(4) because subsection (a)(2)(C) could apply to situations that Nosal suggests are innocuous. Defining the contours of subsection (a)(2)(C) may in fact be difficult. But that is not the task in this case. Password sharing with the intent to defraud is a crime.

CONCLUSION

The CFAA protects the important interests of owners of protected computers, most notably rights of privacy, access, and control over persons' own computers. Nosal proposed two rules — a technical access barrier and a privilege when using a shared password — that would undermine these interests. This Court should reject these theories and affirm the conviction.

Dated: March 9, 2015

Respectfully submitted,

/s/
David Nied
Keenan W. Ng
Michael S. Dorsi
AD ASTRA LAW GROUP, LLP
Counsel for *Amicus Curiae*
NOVELPOSTER

CERTIFICATE OF COMPLIANCE

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 Respondent complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because the brief contains ** 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: March 9, 2015

Respectfully submitted,

/s/
David Nied
Keenan W. Ng
Michael S. Dorsi
AD ASTRA LAW GROUP, LLP
582 Market Street, Suite 1015
San Francisco, CA 94104
Telephone: (415) 795-3579
Facsimile: (415) 276-1976

Counsel for *Amicus Curiae*
NOVELPOSTER

CERTIFICATE OF SERVICE

I hereby certify 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 March 9, 2015.

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

Dated: March 9, 2015

Respectfully submitted,

/s/ ________________________________
David Nied

Counsel for *Amicus Curiae*
NOVELPOSTER