NO. 10-10038

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellant,

v.

DAVID NOSAL,
Defendant-Appellee.

On Appeal from the United States District Court
For the Northern District of California
NO. CR 08-0237 MHP

BRIEF OF AMICUS CURIAE ORACLE AMERICA INC. IN SUPPORT OF THE UNITED STATES

Geoffrey M. Howard
BINGHAM MCCUTCHEN LLP
Three Embarcadero Center
San Francisco, CA 94111
(415) 393-2000

David B. Salmons
Bryan M. Killian
BINGHAM MCCUTCHEN LLP
2020 K Street N.W.
Washington, DC 20006
(202) 373-6000

Attorneys for Amicus Curiae Oracle America Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1, Oracle America Inc. states that it is a wholly owned subsidiary of Oracle Corp., which is a publicly traded corporation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

LEGISLATIVE HISTORY

TABLE OF AUTHORITIES
(continued)

Page(s)

OTHER AUTHORITIES

STATEMENT OF THE AMICUS CURIAE

Oracle America Inc. is one of the world's largest providers of enterprise hardware and software systems and uses computers and networks to serve customers across the globe. Oracle invests heavily in computer and information security. Even so, from time to time, persons who lack or abuse authorization try to access Oracle's computers and information for harmful purposes.

Civil sanctions do not always deter those wrongdoers. Some see civil liability as a cost of doing business. Others are judgment-proof. Thus, prosecutions under laws like the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, are vital to deter and punish illicit behavior.

Oracle knows this firsthand. Between 2005 and 2007, employees of TomorrowNow, Inc. (a subsidiary of one of Oracle's largest competitors in the enterprise applications software business, SAP), accessed Oracle's servers without authorization: using the login credentials of customers, TomorrowNow stole Oracle's software in order to steal Oracle's customers and, hence, its software and support revenues. About three months ago, the United States successfully prosecuted TomorrowNow for eleven counts of accessing computers without authorization or in excess of authorization under subsection (a)(4) of the CFAA—the same subsection at issue in Nosal's

case. *See* Plea Agreement, *United States v. TomorrowNow, Inc.*, No. CR 11-00642 (N.D. Cal. Sept. 14, 2011).

Oracle has a strong interest in the correct interpretation of the CFAA. And given that its headquarters and many of its computers are located in the Ninth Circuit, Oracle also has a strong interest in this Court's correct interpretation of the law. Oracle submits this brief to help the *en banc* Court understand that the CFAA is an important prosecutorial tool, that common-law trespass doctrines apply to the CFAA, and that the concerns about vast criminal liability, expressed by Nosal and his amicus, are overblown.[1]

INTRODUCTION

After leaving the employ of Korn/Ferry International, David Nosal allegedly enticed three of his former coworkers to access the company's computers and download trade secrets to help him start a competing business. Korn/Ferry had authorized those employees to access its computers and trade secrets, but only for legitimate Korn/Ferry business; it forbade access for any other purpose. For his alleged role as mastermind, aider, and abettor of the scheme, Nosal was charged with violating subsection (a)(4) of the

[1] Pursuant to Rule 29(c)(5), Oracle states that neither party's counsel authored any of this brief and that Oracle alone paid to prepare and submit it. Counsel for the United States and counsel for Nosal have consented to the filing of this brief.

CFAA, which makes it a crime for any person, "knowingly and with intent to defraud, [to] access[] a protected computer without authorization, or [to] exceed[] authorized access, and by means of such conduct further[] the intended fraud and obtain[] anything of value." 18 U.S.C. § 1030(a)(4).

Nosal urges the Court to hold that subsection (a)(4) does not cover the alleged conduct. He argues that subsection (a)(4) and other similarly worded subsections of the CFAA narrowly prohibit just two discrete forms of access not alleged here: accessing a computer without any authorization whatsoever ("access[ing] a protected computer without authorization") and accessing certain information on a computer when limited authorization was given to access only other information ("exceed[ing] authorized access"). In his view, the CFAA backs a computer owner's decision to wall off computers and information from access altogether, but not the decision to offer restricted access, *i.e.* access for some purposes but not others. Otherwise, Nosal contends, the CFAA would be unconstitutional: because so many people use work computers for personal reasons and ignore the terms of use for Internet websites, nearly everyone would be a criminal and enforcement would be arbitrary.

Nosal's interpretation of the CFAA lacks merit. As the Government shows and as the panel majority and other courts have held, the text of the

CFAA reaches access that violates any restriction an owner imposes—including restrictions that limit access to company business, not competing business. Legislative history confirms that was Congress's goal.

The key to understanding why the Government's interpretation of the CFAA is neither surprising nor unduly broad is in recognizing that Congress rooted the CFAA in common-law trespass doctrines. Among them is the concept of restricted authorization: a person commits trespass not only when he or she enters property or a portion of it when told not to; a person commits trespass also when he or she has authorization to enter for some purposes but enters for different ones. Over the many centuries trespass has been a crime and a tort, even though liability has turned on owners' personal decisions whether and to what extent to authorize entry, liability has not run amok because courts have developed rules to cabin it. Applied to the CFAA, those well established rules defeat Nosal's contention that millions of Americans violate the CFAA under the Government's interpretation.

In short, the panel majority was correct, and the *en banc* Court should not adopt Nosal's limiting construction of the CFAA.

ARGUMENT

I. THROUGH THE CFAA, CONGRESS ADAPTED COMMON-LAW TRESPASS PRINCIPLES TO COMPUTERS.

"There are countless situations in which the State prohibits conduct only when it is objected to by a private person most closely affected by it." *Planned Parenthood of Missouri v. Danforth*, 428 U.S. 52, 93 n.1 (1976) (White, J., concurring in part). One of those situations is trespass, *id.*, the essence of which is entry onto property without the owner's consent, *see* Restatement (Second) Torts §§ 158, 167 (1965). Governments have long enforced trespass criminally. In fact, though best known today as a tort, trespass was first a crime "because the trepasser's conduct was regarded as a breach of the peace." 75 Am. Jur. 2d, *Trespass* § 1. *See* Prosser & Keeton, *Torts* § 6, at 29 (5th ed. 1984).

In a variety of contexts, modern statutes, civil and criminal alike, build upon the foundation of common-law trespass. *See* Model Penal Code Commentaries § 221.2 (1980) (listing various criminal trespass statutes). Trespass is a particularly "logical starting point for applying property crimes to punish and deter computer misuse." Kerr, *Cybercrime's Scope*, 78 N.Y.U. L. Rev. 1596, 1606 (2003). For "[t]he essence of trespass, unlawful entry, corresponds quite neatly to unauthorized accessing of electronic prop-

erty." Olivenbaum, *Rethinking Federal Computer Crime Legislation*, 27 Seton Hall L. Rev. 574, 640 (1997).

The Congresses that enacted and amended the CFAA began with trespass, too. "The basic legal concept underlying the CFAA is the concept of 'unauthorized access,' a concept derived from the idea of trespass." Winn, *The Guilty Eye*, 62 Bus. Law. 1395, 1403 (2007). The legislative history of the CFAA is replete with signs that trespass is the law's foundation. *See* 131 Cong. Rec. S11,872 (daily ed. Sept. 20, 1985) ("The conduct proscribed in [this section] is akin to a trespass onto someone else's property."); S. Rep. No. 99-432, at 7 (1986) (using "trespass" as shorthand for unauthorized access); S. Rep. No. 104-357, at 10–11 (1996) (same).

More importantly, the text of the CFAA is obviously modeled on common-law trespass. Replace "access" with "entry" and "computer" with "property," and subsection (a)(4) of the CFAA sounds exactly like it prohibits ordinary trespass: "Whoever … enters property without authorization, or exceeds authorized entry, … shall be punished … ." *Compare Holland Livestock Ranch v. United States*, 655 F.2d 1002, 1005 (9th Cir. 1981) ("A grazing trespass exists when livestock are grazed on federal public land *in excess of* authorized permit use or *without* an appropriate permit or license." (emphases added)).

When Congress uses common-law terms in a statute, as it has in the CFAA, Congress "adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken." *Carter v. United States*, 530 U.S. 255, 264 (2000) (quoting *Morissette v. United States*, 342 U.S. 246, 263 (1952)) (internal quotation marks omitted). Therefore, the Court must look to the common law's understanding of "authorization" in interpreting the CFAA. This is not a novel approach. In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), this Court held that the CFAA and the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, another federal statute related to computer access, should be interpreted in light of common-law trespass principles. *Theofel* was a civil suit where the two sides disputed whether the defendant's access had been validly authorized when the defendant had obtained authorization deceitfully. *See* 359 F.3d at 1072. After recognizing that the Stored Communications Act had the trappings of a trespass statute, the Court looked to the common law of trespass to resolve the dispute and held that, as alleged, the authorization was invalid. *Id.* at 1072–1074. The Court also held that its analysis of authorization under the Stored Communications Act "disposed of" the same issue under the CFAA. *Id.* at 1078.

Although the primary legal question in Nosal's case (*i.e.* what kinds of access restrictions does the CFAA enforce) is different from the question in *Theofel* (*i.e.* when will courts imply access restrictions the owner has not made express), there is no doubt the *en banc* Court should follow *Theofel*'s lead and look to the common law of trespass for the answer. And as shown below, the interpretation of the CFAA advanced by the Government and accepted by the panel majority accords with the established common-law rule that a person commits a trespass when he violates *any* access restriction a property owner imposes—including access restricted for certain purposes.

II. THE COMMON LAW OF TRESPASS RECOGNIZES THAT OWNERS CAN GRANT RESTRICTED ACCESS TO THEIR PROPERTY.

A. Courts recognize many types of restrictions on access.

No one disputes that the CFAA places the weight of criminal penalties behind a computer owner's decision to withhold all access to his computers. The dispute in this case is over the extent to which the CFAA backs other access restrictions with criminal penalties. Without mentioning the common law of trespass, Nosal argues that the CFAA enforces only one specific type of access restriction—authorization to access some but not all information on a computer. *See* Nosal Reh'g Pet. at 7. Accordingly, Nosal argues that the CFAA does not make it a crime for a person who has authorization to

access a computer or information *for business purposes only* to access the same computer or information for the decidedly non-business purpose of stealing information to use in competition with the computer owner.

The common law of trespass does not distinguish among types of access restrictions. It recognizes them all. The Restatement is clear: "A … restricted consent to enter land creates a privilege to do so *only in so far as the … restriction is complied with*." Restatement (Second) Torts § 168 (1965) (emphasis added).[2] It follows that "consent restricted to entry for a particular purpose confers no privilege to be on the land for any other purpose." *Id.* § 168 cmt. *b*. Similarly, "[o]ne may become a trespasser by exceeding the scope of consent, such as by intentionally conducting oneself in a manner differing from that allowed." 75 Am. Jur. 2d, *Trespass* § 75.

For example, a land owner can limit access to certain areas of a property and can limit access to certain times. *See* Restatement (Second) Torts §§ 169, 170 (1965). If someone immediately enters a forbidden area or enters outside the allotted window, he or she enters without authorization. If

[2] The Restatement refers to both "conditional consent" and "restricted consent," defining them differently but treating them the same. *Compare* Restatement (Second) Torts § 892A cmt. *f* (1979) (defining "conditional consent" as consent "effect only upon the occurrence or nonoccurrence of an event or the existence of nonexistence of a fact"), *with id.* § 892A cmt. *g* (defining "restricted consent" as consent limited "to acts done for a particular purpose"). For simplicity, this brief refers only to "restricted consent."

someone roams outside authorized areas or stays too long, he or she exceeds authorization. Either way, the person is a trespasser. Thus, contrary to Nosal's amicus, *see* Electronic Frontier Foundation Amicus Br. in Support of Reh'g at 13–14 (hereinafter, "EFF Reh'g Br."), the common law of trespass amply supports the Government's view that the CFAA may criminalize accessing medical records after business hours when the computer owner has limited access of the records to times during business hours, *see* Gov't Reply Br. at 8–9.

The common law of trespass also answers the precise question posed in this case: owners also can restrict access according to a person's purpose. Not only does this mean that an owner can authorize entry only to perform a particular activity. *See* Restatement (Second) Torts § 168 illus. 1 (it is a trespass to draw gravel from Blackacre when authorized only to drive cattle across Blackacre). But it also means that an owner can authorize entry only to perform a particular activity *and only for a particular purpose*. *See id.* § 168 illus. 3 ("A grants permission to B, his neighbor, to enter A's land and draw water from A's spring for B's own use. A has specifically refused permission to C to enter A's land and draw water from the spring. At C's instigation, B enters A's land and obtains for C water from the spring. B's entry is a trespass.").

The analogy from common-law trespass to computer access under the CFAA is straightforward. If a computer owner authorizes a customer to access a computer only to download software updates for an older software release, the CFAA prohibits that person from accessing the computer to download a brand new release. Moreover, if a computer owner authorizes a customer to access a computer only to download software updates and only for the customer's own noncompeting purposes, the CFAA prohibits that person from accessing the computer in order to sell the updates to others or use them to compete with the computer owner.

Nosal's amicus argues that interpreting the CFAA to back any access restriction a computer owner imposes effectively makes the fraudulent-intent element of subsection (a)(4) superfluous. *See* EFF Reh'g Br. at 10. Not so. Trespass is not inherently fraudulent. *See, e.g.*, *Food Lion, Inc. v. Capital Cities / ABC Inc.*, 194 F.3d 505, 514, 519 (4th Cir. 1999) (reversing fraud verdict and affirming trespass verdict). To establish fraud, the evidence must show that the accesser concealed the activity, disguised his or her identity, or made misrepresentations. *See United States v. Rogers*, 321 F.3d 1226, 1230 (9th Cir. 1993). Sometimes, the same evidence will establish lack of authorization and fraud, like when the accesser uses someone else's login credentials. But that result is not inevitable.

B. A person's post-access conduct can show that he violated a computer owner's restrictions on access.

Noting that the text of the CFAA focuses on "access," Nosal argues that a person's post-access conduct should be totally immaterial to CFAA liability. He claims that computer owners "can define the permissible scope of *access* to information but not the permissible scope of *subsequent use* of that information." Nosal Reh'g Pet. at 8. *See* EFF Reh'g Br. at 9, 11. Nosal's dichotomy is fatally oversimplified.

While *accessing* and *using* information are indeed two separate acts, they are not so logically separate that post-access use is totally immaterial to determining the propriety of the initial access. On the contrary, because a person's purpose at the time of access is so hard to prove, "[t]he fact that the improper purpose is in fact carried out is itself evidence that the entry was for that purpose, and may be conclusive in the absence of any explanation for a change in plan." Restatement (Second) Torts § 892A cmt. *g* (1979).

III. MILLIONS OF AMERICANS WILL NOT BE CRIMINALS IF THE COURT INTERPRETS THE CFAA IN LIGHT OF THE COMMON LAW OF TRESPASS.

The unlikely prospect of limitless criminal liability animates this case. Nosal imagines that, unless the Court construes the CFAA to criminalize only access that involves computers or information a person is categorically forbidden to access, "tens of millions" of employees will be criminals. No-

sal Reh'g Pet. at 10. Supposedly, "millions of employees … violate their employers' computer use restrictions every day," and "millions of Internet users" will be turned "into criminals for typical, routine Internet activity." EFF Reh'g Br. at 11, 15.

To dispel those concerns, the Government and the panel majority point to the heightened *mens rea* requirement of subsection (a)(4), which proscribes accessing a computer without authorization or exceeding authorized access "knowingly and with intent to defraud." 18 U.S.C. § 1030(a)(4). Nosal counters that other CFAA subsections, particularly subsection (a)(2), are not limited to cases of fraud but cover access done "intentionally." *See* Nosal Reh'g Pet. at 9–12; *see also* EFF Reh'g Br. at 12–13. Other CFAA subsections do have different *mens rea* requirements, but Nosal is wrong to conclude that millions of people therefore violate those subsections every day. Nosal's sky-is-falling assertion of vast criminal liability relies on a flawed premise—the assumption that an employee accessing a computer in ways an employee handbook forbids or a person accessing a website contrary to the site's posted terms of use is inherently accessing a computer without or in excess of authorization. *See* EFF Reh'g Br. at 15–18 (concocting a parade of horribles from selected Internet website terms of service). At common law, trespass liability is not so simplistic.

Courts applying the common law of trespass recognize that consent is a "willingness in fact for conduct to occur." Restatement (Second) Torts § 892(1) (1979). It is a fact-dependent conclusion drawn from the totality of the circumstances, and "it may be manifested by action or inaction and need not be communicated to the actor." *Id.*; *see id.* § 892 cmt. *c*. Accordingly, courts sometimes find that a written or posted access restriction has been overridden or lifted.

This common-law principle takes several forms. One is the doctrine of apparent or implied consent; another is estoppel or waiver. Courts are suspicious of posted access restrictions that *by their terms* apply to everyone but that *in fact* have been selectively enforced "against some members of the public as opposed to others"; when the signals conflict, courts may find a posted restriction ineffective. Winn, *The Guilty Eye*, 62 Bus. Law. at 1424. Similarly, a property owner who knowingly acquiesces in a person's course of access may waive the right to call it a trespass. *See id.*; *see also* 75 Am. Jur. 2d, *Trespass* § 67 (estoppel defense). When an owner has "actual knowledge" of repeated trespasses, the owner's "habitual acquiescence … may constitute a license for persons to enter the land, if the tolerance is so pronounced as to be tantamount to permission." 75 Am. Jur. 2d, *Trespass* § 73. Community custom is especially relevant in determining apparent

consent. *See* Restatement (Second) Torts § 892 cmt. *d*; *cf. McKee v. Gratz*, 260 U.S. 127, 136 (1922) ("A license may be implied from the habits of the country."). Above all, commonsense and reasonableness are the guides, as they are with all totality-of-the-circumstances inquiries.

Like other established doctrines of the common law of trespass, the reasonable approach to judging posted access restrictions applies to the CFAA. And it easily answers Nosal's policy concerns. If, as Nosal posits, it is well known that millions of employees and Internet users actually violate posted restrictions on computer and information access every day, chances are good that those restrictions are not bona fide. That result is not far-fetched; just last year, in fact, Nosal's amicus told the Supreme Court that "many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency." *Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010). Given how often and how openly those posted yet never enforced restrictions are violated, a person who violates one is not accessing a computer without or in excess of authorization.

IV. CONGRESS HAS DETERMINED THAT A COMPUTER OWNER'S RIGHT TO CONTROL ACCESS IS IMPORTANT ENOUGH TO WARRANT CRIMINAL PENALTIES.

Nosal's characterization of the policy consequences of this case makes it seem as if the Government, employees, and Internet users are the

only stakeholders in the CFAA. There are many more. "Firms and individuals invest substantial amounts of capital and effort to create servers and websites that are linked to the rest of cyberspace via the internet." Epstein, *Cybertrespass*, 70 U. Chi. L. Rev. 73, 79 (2003). The CFAA is the culmination of years of effort by several Congresses to balance the interests of computer users with those of computer owners. The CFAA's criminal penalties are a particularly important part of Congress's goal of maintaining privacy and preventing unwanted computer access.

The common law makes clear that self-help is a poor remedy for trespass. Self-help is usually neither effective nor efficient. Fences can go only so high and walls only so thick. And there often is much good to be gained from allowing some people to access land for some purposes, as opposed to keeping everyone out. The same is true for computers and networks. As long as one person has authorization to access a computer for good and useful reasons, it is possible for someone—even that person—to access the computer for other reasons.

Civil liability does not always prevent improper computer access. Deep pockets see paying civil damages for the harm their access causes as a cost of doing business. Shallow and empty pockets (including many hackers and snoops), on the other hand, are judgment-proof. Even when an owner

can collect, damages often do not compensate for the whole harm. Like other laws that protect against trespass, the CFAA protects privacy. *Cf. Theofel*, 359 F.3d at 1072 (noting that "the Stored Communications Act protects individuals' privacy and proprietary interests"). Invasions of privacy, unaccompanied by demonstrable harm to another legally protected interest, are not easily assigned a dollar value. Because "[n]o one in his right mind sues for nominal damages," "[o]ne dividend of strong trespass rules is that they protect the privacy of the property owners." Epstein, *Cybertrespass*, 70 U. Chi. L. Rev. at 75, 78.

Interpreting the CFAA as Nosal does would defeat this core purpose. If Nosal prevails, criminal penalties would be limited only to cases where the person who accesses a computer or information is categorically forbidden ever to access that computer or information. Thieves would have an easy-to-follow roadmap for avoiding criminal penalties—enlist the help of an employee, customer, or other person with restricted authorization to access the computer or the information the thief wants to access. Congress reasonably decided not to have the CFAA turn on whether a thief works alone or with a pawn. *Cf. Theofel*, 359 F.3d at 1074 (rejecting an interpretation of "authorization" under the Stored Communications Act that would

have exempted intrusions that "seem the paradigm of what [Congress] sought to prohibit").

The *en banc* Court therefore should not accept Nosal's invitation to interpret the CFAA so narrowly as to defeat one of its core purposes.

CONCLUSION

For the foregoing reasons, the *en banc* Court should hold that the common law of trespass applies to the CFAA and that the District Court erred in dismissing the Government's case against Nosal.

Respectfully submitted,

Dated: December 1, 2011

/s/ Geoffrey M. Howard

David B. Salmons
Bryan M. Killian
BINGHAM MCCUTCHEN LLP
2020 K Street N.W.
Washington, DC 20006
(202) 373-6000

Geoffrey M. Howard
BINGHAM MCCUTCHEN LLP
Three Embarcadero Center
San Francisco, CA 94111
(415) 393-2000

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because:

__X__ this brief contains 3,862 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), *or*

_____ this brief uses a monospaced typeface and contains _____ lines of text, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

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:

__X__ this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2003 in 14 Point Times Roman, *or*

____ this brief has been prepared in a monospaced typeface using *[state name and version of word processing program]* with *[state number of characters per inch and name of type style]*.

/s/ Geoffrey M. Howard
Geoffrey M. Howard

CERTIFICATE OF SERVICE

I hereby certify that on this 1st day of December 2011, a copy of the foregoing Brief of Amicus Curiae Oracle America Inc. in Support of the United States was served by CM/ECF on all participants in the case.

/s/ Geoffrey M. Howard
Geoffrey M. Howard