No. 16-

IN THE
Supreme Court of the United States

DAVID NOSAL,
Petitioner,
v.

UNITED STATES OF AMERICA
Respondent.

On Petition for a Writ of Certiorari to the
United States Court of Appeals
for the Ninth Circuit

PETITION FOR A WRIT OF CERTIORARI

THOMAS P. SCHMIDT
HOGAN LOVELLS US LLP
875 Third Avenue
New York, NY 10022

DENNIS P. RIORDAN
TED SAMPSELL-JONES
RIORDAN & HORGAN
523 Octavia Street
San Francisco, CA 94102

NEAL KUMAR KATYAL
Counsel of Record
EUGENE A. SOKOLOFF
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5600
neal.katyal@hoganlovells.com

Counsel for Petitioner

QUESTION PRESENTED

The Computer Fraud and Abuse Act ("CFAA") imposes civil and criminal penalties on anyone who "accesses a computer without authorization" or who "exceeds authorized access." 18 U.S.C. § 1030(a). But three decades' experience with the statute has failed to produce any consensus on *whose* authorization matters.

In this case, the Ninth Circuit held that a computer's owner has exclusive discretion to authorize access—an account holder cannot independently confer authorization. That tracks the approach adopted by the First, Fifth, and Seventh Circuits, which define authorization in terms of the computer owner's intentions, expectations, and contractual or agency relationships. But it splits sharply with the Second and Fourth Circuits, which reject such factors as irrelevant and instead construe the CFAA narrowly as an anti-hacking statute.

The question presented is:

Whether a person who obtains an account holder's permission to access a computer nevertheless "accesses a computer without authorization" in violation of the CFAA when he acts without permission from the computer's owner.

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

Page(s)

CASES:

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

IN THE
Supreme Court of the United States

No. 16-

DAVID NOSAL,
Petitioner,
v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for a Writ of Certiorari to the
United States Court of Appeals
for the Ninth Circuit

PETITION FOR A WRIT OF CERTIORARI

Petitioner David Nosal respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit in this case.

OPINIONS BELOW

The Ninth Circuit's original opinion is reported at 828 F.3d 865. The Ninth Circuit's amended opinion is reported at 844 F.3d 1024. Pet. App. 1a-70a. The District Court's order denying petitioner's motions for a new trial and for acquittal is unreported but available at 2013 WL 4504652. Pet. App. 71a-138a. The District Court's order denying petitioner's motion to dismiss the indictment is reported at 930 F. Supp. 2d 1051. Pet. App. 139a-163a.

JURISDICTION

The Ninth Circuit entered judgment on December 8, 2016. That same day, the Court of Appeals denied a timely petition for rehearing en banc. On February 24, 2017, Justice Kennedy granted petitioner's timely application to extend the time for filing a petition for a writ of certiorari to and including April 7, 2017. On March 24, 2017, Justice Kennedy granted petitioner's application to further extend the time to and including May 5, 2017. This Court has jurisdiction under 28 U.S.C. § 1254(1).

STATUTE INVOLVED

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is reproduced in an appendix to this petition. Pet. App. 164a-167a.

INTRODUCTION

This case presents one of the most important and recurring questions in an age of networked computing: When does someone have permission to access someone else's computer? Any time a person logs in to their office computer or signs in to their Gmail or Facebook account, she "accesses" computers belonging to her employer, or the website's or service's owner. In this case, a divided panel of the Ninth Circuit held that doing any of those things without the owner's permission violates a federal criminal statute, the Computer Fraud and Abuse Act ("CFAA").

The panel majority's ruling puts it at the extreme end of a 4-2 circuit split. On one side, the First, Fifth, Seventh, and Ninth Circuits look to the owner's intentions, expectations, and contractual or agency relationships to determine whether access to

a computer is "authorized" under the statute. On the other side, the Second and Fourth Circuits reject such factors as irrelevant.

The Ninth Circuit's decision exposes a broad range of innocuous, day-to-day activity to criminal prosecution. If a computer's owner has exclusive discretion to grant or revoke authorization, a person could violate the statute any time he logged in to a computer in violation of the owner's policies or terms of service. Take, for example, a person who uses his spouse's password to log into the family's online banking account to pay a bill. Or an assistant who logs into an executive's email account to print out a presentation. If the banking and email services prohibit password-sharing, the Ninth Circuit's reasoning would transform these quotidian acts into violations of the CFAA, punishable by a fine and up to a year in prison, even if the users had no criminal intent.

Because the Ninth Circuit's decision exacerbates a deep division among the courts of appeals over the scope of an important federal criminal statute, and because the decision massively and unpredictably expands the scope of liability, this Court should grant review.

STATEMENT

A. Statutory Background

Congress originally enacted the CFAA in 1984 in response to the "advent of the activities of so-called 'hackers' who have been able to access (trespass into) both private and public computer systems." H.R. Rep. No. 98-894, at 10 (1984). Hackers, the House Judiciary Committee warned in proposing a subsequent amendment, "are trespassers, just as much as

if they broke a window and crawled into a home while the occupants were away." H.R. Rep. 99-612, at 5-6 (1986). "The conduct prohibited" by the CFAA was thus "analogous to that of 'breaking and entering' rather than using a computer * * * in committing the offense." H.R. Rep. 98-894, at 20 (1984); *see* S. Rep. 99-432, at 9 (1986).

The CFAA criminalizes accessing a computer "without authorization" or "exceeding authorized access." 18 U.S.C. § 1030(a). It also provides for private civil actions for damages. *Id.* at § 1030(g). The subsection at issue in this case punishes whoever "knowingly, and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access." *Id.* at § 1030(a)(4). The statute also prohibits "obtain[ing] * * * information" without authorization, regardless of culpable intent. *Id.* at § 1030(a)(2)(C). These provisions apply to any "protected computer," defined as a computer "which is used in or affecting interstate or foreign commerce or communication." *Id.* at § 1030(e)(2)(B). And the term "computer" is itself broadly defined to include, among other things, "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions." *Id.* at § 1030(e)(1). In other words, the statute reaches virtually any device connected to the Internet.

B. Factual And Procedural Background

1. David Nosal worked for Korn/Ferry International, a global executive search firm. As part of its business, Korn/Ferry maintained a database of prospective executive candidates. Pet. App. 6a-8a.

Employees used this database to identify potential placements. *Id.*

In 2004, Nosal left Korn/Ferry to start his own search firm. *Id.* at 6a. Nosal was joined in early 2005 by two former colleagues. *Id.* at 7a. Before they left Korn/Ferry, Nosal's colleagues downloaded material from the company's database. Pet. App. 8a. And, in the months following their departure, Nosal's colleagues asked Nosal's former assistant at Korn/Ferry to lend them her credentials so that they could continue to access the database. *Id.* at 8a-9a. Alerted to this activity, Korn/Ferry launched an internal investigation and eventually persuaded federal authorities to initiate criminal proceedings. *Id.* at 9a.

2. The Federal Government indicted Nosal in 2008 on a series of charges, including eight counts under the CFAA, 18 U.S.C. § 1030(a)(4). Nosal moved to dismiss the CFAA counts on the ground that the statute prohibits hacking into a computer, not misappropriating information. The District Court granted Nosal's motion in part and denied it in part. It dismissed five CFAA counts that were based on Nosal's colleagues' use of their own credentials to download information from Korn/Ferry's database while they were still Korn/Ferry employees—the "own-password" counts. But it denied Nosal's motion as to the three remaining counts, which were based on occasions when Nosal's colleagues used the password of his former assistant to access the database after they had left the firm—the "password-sharing" counts. The Government filed an interlocutory appeal, *see* 18 U.S.C. § 3731, and the Ninth Circuit eventually affirmed en banc. *See United States* v.

Nosal, 676 F.3d 854 (9th Cir. 2012) (Kozinski, J.) ("*Nosal I*").[1]

The Court of Appeals explained that the CFAA's "purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets." *Id*. at 863. It rejected the Government's contention that Nosal's colleagues "exceed[ed] authorized access" when they downloaded information in violation of Korn/Ferry policy. *Id*. at 864. The court warned that adopting such an interpretation of the statute would "expand [the CFAA's] scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer." *Id.* at 859.

3. On remand from *Nosal I*, the Government filed a second superseding indictment that charged the three password-sharing CFAA counts, two counts of trade secret theft under the Economic Espionage Act ("EEA"), 18 U.S.C. § 1832, and one conspiracy count. Pet. App. 10a. The District Court denied Nosal's renewed motion to dismiss the password-sharing counts. It found that *Nosal I* had not "explicitly h[e]ld that the CFAA is limited to hacking crimes." *Id.* at 156a. Even if it had, the District Court concluded that the indictment sufficiently alleged "circumvention of technological access barriers" by alleging that Nosal's colleagues had accessed Korn/Ferry's database by entering a borrowed password. *Id.* at 157a. The case proceeded to trial.

---

[1] Circuit precedent barred Nosal from cross-appealing the District Court's refusal to dismiss the password-sharing counts. *See United States* v. *Fort*, 472 F.3d 1106, 1121 (9th Cir. 2007).

Nosal asked that the jury be instructed that "[a] person accesses a computer without authorization when he circumvents technological access barriers." C.A. E.R. 1083; *see id*. at 109. The District Court refused. Instead, the court told the jury that it was up to Korn/Ferry "to grant or deny permission to [a] person to use the computer" and that "[a] person uses a computer 'without authorization' when the person has not received permission from Korn/Ferry to use the computer for any purpose * * * or when Korn/Ferry has rescinded permission to use the computer." *Id.* at 109. The jury returned a verdict of guilty on all counts and the District Court denied Nosal's motions for acquittal and for a new trial. Pet. App. 10a.

The jury was also instructed that, if Nosal was guilty of conspiracy, he was liable under each of the other counts, so long as the jury found that one of his alleged co-conspirators had committed the charged offense and that it furthered the conspiracy's purpose. *See* C.A. E.R. 106-107; *Pinkerton* v. *United States*, 328 U.S. 640, 646-648 (1946). Because the jury entered a general verdict on the conspiracy count, it is not clear whether it found that the conspiracy's purpose was to misappropriate trade secrets (in violation of the EEA) or to gain unauthorized access to a computer (in violation of the CFAA). Jury Verdict 1, *United States* v. *Nosal* (N.D. Cal. No. 3:08-cr-00237), Doc. 408. The Government did not dispute below that this general verdict means that, if the courts below misconstrued the elements of the CFAA, Nosal's convictions on all counts must be vacated. *See* Pet. App. 69a-70a n.17 (Reinhardt, J., dissenting).

4. A divided panel of the Ninth Circuit affirmed. In an amended opinion issued after the court denied Nosal's petition for rehearing en banc, the panel majority concluded that "Korn/Ferry owned and controlled access to its computers, including the [company's] database, and it retained *exclusive discretion to issue or revoke access* to the database." *Id.* at 19a (emphasis added). "Implicit in the definition of authorization," the majority explained, "is the notion that someone, including an entity, can grant or revoke that permission." *Id.* at 18a. The majority found that "[h]ere, that entity was Korn/Ferry." *Id.* Accordingly, it held that Nosal "acted 'without authorization'" when his colleagues accessed Korn/Ferry's database using a borrowed password after the company had "affirmatively revoked" his credentials when he left his job. *Id.* at 24a. The court used that same reasoning to reject Nosal's challenge to the District Court's jury instruction making owner permission the sole determinant of "authorization." *Id.* at 24a-26a. The majority went on to reject Nosal's challenges to the EEA and conspiracy counts. *Id.* at 26a-40a. But it vacated and remanded the District Court's restitution award. *Id.* at 41a-47a.

Judge Reinhardt dissented. He warned that the majority's opinion "loses sight of the anti-hacking purpose of the CFAA" and "threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens." *Id.* at 49a (Reinhardt, J., dissenting). "The question that matters," Judge Reinhardt argued, "is not what authorization *is* but who is entitled to give it." *Id.* at 56a. Because the statute is ambiguous on that score, Judge Reinhardt would have applied the rule of lenity and "adopt[ed] [a]

construction of CFAA that criminalizes access only by those without permission from *either* an account holder *or* the system owner." *Id.* at 58a-59a.

This petition followed.

REASONS FOR GRANTING THE PETITION

The Ninth Circuit's construction of the CFAA threatens to criminalize a broad swath of innocuous activity that ordinary people engage in every day. That alone is reason enough for this Court's immediate review. The decision also deepens longstanding confusion among the circuits over who may authorize access under the CFAA.

I. THE COURTS OF APPEALS ARE DIVIDED OVER WHO MAY AUTHORIZE ACCESS UNDER THE CFAA

The panel majority held that a computer's owner has "*exclusive* discretion" to "issue or revoke access" under the CFAA. Pet. App. 19a (emphasis added). The nation's largest Circuit, the Ninth, thus joins the First, Fifth, and Seventh in defining authorization in terms of a computer owner's intentions, expectations, and contractual or agency relationships. That contradicts the views of the Second and Fourth Circuits that such factors are irrelevant. So while a person who logs in to a computer account using a borrowed password against the owner's wishes commits a federal crime in the First, Fifth, Seventh, and Ninth Circuits, proof of the same conduct would not establish CFAA liability in the Second and Fourth Circuits.

1. Start with the Second and Fourth Circuits: Those courts have construed the CFAA narrowly as an anti-hacking statute that bars only the computer

equivalent of breaking and entering. They categorically reject any inquiry into the owner's policies or preferences. The conduct alleged in this case could not satisfy that standard because, whatever Korn/Ferry's relationship with Mr. Nosal may have been, Nosal's former assistant voluntarily lent her valid access credentials to his colleagues.

a. In *WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F.3d 199 (4th Cir. 2012), the Fourth Circuit equated authorization with the practical ability to access a computer. The court explained that "an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer." *Id*. at 204. But the court understood approval in a narrow sense. It held that even though the defendant plainly violated his employer's policies when he downloaded company information to benefit a competitor, his acts were "authorized" because he "had *access* to [the plaintiff's] intranet and computer servers." *Id.* at 206-207 (emphasis added) (citing 18 U.S.C. § 1030(a)(2)(C), (a)(4), (a)(5)(B)-(C)). In other words, the employer broadly "authorized" the defendant to access its computers by providing him with the *means* to access them.

The Fourth Circuit's reasoning suggests that authorized access, like the key to an apartment, can be shared with third parties. After all, *WEC Carolina* never specifies *whose* "permission" is required. *Id.* at 206; *see* Pet. App. 56a (Reinhardt, J., dissenting). An owner "might choose to rescind" authorization if a user shares access. *WEC Carolina*, 687 F.3d at 206. But it can do so only by changing the locks; a violation of access rules does not void the authorization. *Id.* at 206-207.

b. The Second Circuit took a similar approach in *United States* v. *Valle*, 807 F.3d 508 (2d Cir. 2015), reversing a conviction for "exceed[ing] authorized access" based on a police officer's use of a law enforcement database without a "law enforcement purpose." *Id.* at 523. The court concluded that the rule of lenity required reading the CFAA to prohibit only "hacking" offenses analogous to criminal trespass or "breaking and entering." *Id.* at 525 (quoting H.R. Rep. No. 98-894, at 3706); *see id.* at 524-526. It rejected the Government's argument that liability depends on "fact-specific questions" such as "whether the applicable authorization was clearly defined and whether the abuse of computer access was intentional." *Id.* at 528 (internal quotation marks omitted). Because the officer had access to the information he viewed, he was "authorized" to view it, even though he "violated the terms of his employment by putting his authorized computer access to personal use." *Id.* at 523 (citing 18 U.S.C. § 1030(a)(2)(B)).

The Second Circuit's decision—and its references to "hacking" and "breaking and entering"—suggest that access is "authorized" so long as it does not breach some technological access barrier. As in *WEC Carolina*, the implication is that a person who uses a borrowed password accesses a computer with the authorization the password itself implies.

2. The Ninth Circuit has now joined the First, Fifth, and Seventh Circuits in looking instead to the computer owner's intentions, expectations, and contractual or agency relationships to determine whether access is authorized. Yet it is the only Circuit to categorically bar account-holder authorization; the First, Fifth, and Seventh Circuits have read "authorization" flexibly, leaving the door open to

password-sharing and other forms of derivative authorization consistent with the owner's interests and reasonable expectations.

a. In *International Airport Centers, L.L.C.* v. *Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit construed "authorization" in light of agency-law principles. The court held that that an employee acted "without authorization" when he deleted incriminating files from his employer-issued laptop. *Id.* at 420 (citing 18 U.S.C. § 1030(a)(5)(A)(ii)). The court reasoned that deleting the information was a "breach of [the employee's] duty of loyalty" that "terminated his agency relationship * * * and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420-421.

Although the agency-based reasoning in *Citrin* limits an account holder's discretion, it would allow an account holder to delegate access to a third party in appropriate circumstances without seeking the owner's consent. *Cf.* Restatement (Third) of Agency § 8.06 (2006) (a principal's consent is required only to negate a breach of duty). The question would center on whether the delegation was consistent with the account holder's duties to the owner. *See Citrin*, 440 F.3d at 420. Thus, for example, an attorney could authorize her assistant to respond to email through her law firm account on her behalf. The assistant's access would be "authorized" in the Seventh Circuit as long as the delegation was "necessary or incidental to achieving the [firm's] objectives." Restatement (Third) of Agency § 2.02 (2006).

b. The Fifth Circuit similarly interprets authorization in light of the "expected norms of intended use,"

without requiring permission from the computer owner. *United States* v. *Phillips*, 477 F.3d 215, 219 (5th Cir. 2007). In *Phillips*, the court of appeals considered whether a student acted "without authorization" when he developed a computer program that accessed confidential data on his university's network. *Id.* at 217-218, 219 (citing 18 U.S.C. § 1030(a)(5)(A)(ii)). The court concluded that running the program "was not an intended use of the [university's] network within the understanding of any reasonable computer user." *Id.* at 220; *see id.* at 220-221; *accord United States* v. *John*, 597 F.3d 263, 271 (5th Cir. 2010).

The Fifth Circuit's "intended-use analysis" opens the door to a wide range of access-sharing. If, for example, a school that issued laptops to its students would "reasonabl[y] expect[]" that parents would occasionally use them, that use would be "authorized" in the Fifth Circuit. *Phillips*, 477 F.3d at 220 (quoting *EF Cultural Travel BV* v. *Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001)) (in parenthetical).

c. Like the Seventh Circuit, the First Circuit considers an account holder's duties to a computer's owner. But it has also suggested, like the Fifth Circuit, that the owner's reasonable expectations matter. The defendant in *EF Cultural Travel* used inside information gleaned from his time as an employee to help develop a program that "scraped" data from his former employer's website. 274 F.3d at 579-580. The court recognized that any member of the public could in theory gather the same data from the site. *Id.* at 583. "Practically speaking, however," only the scraper program, enhanced by the defendant's insider knowledge, could do so effectively. *Id.*

The court thus held that the defendant likely "exceeded authorized access" to the website. *Id*. at 580-581 (citing 18 U.S.C. § 1030(a)(4)); *see Citrin*, 440 F.3d at 420 (noting that the "difference between 'without authorization' and 'exceeding authorized access' is paper thin" if "not quite invisible"). Because the First Circuit's decision rested on the fact that the defendant was prohibited by a confidentiality agreement from using his inside knowledge to develop the scraper, it had no need to "reach the more general arguments made about statutory meaning." *EF Cultural Travel*, 274 F.3d at 581-582. But the court clearly found it relevant that an ordinary user could not easily have obtained the same data from the website. *Id.* at 583; *see also id.* at 582 n.10 (noting the role of intent and expectations in assessing whether access is authorized).

Under the First Circuit's hybrid analysis, a user's access is "authorized" so long as it comports with the user's obligations—if any—to the computer's owner, and with the owner's reasonable expectations. Absent a contractual limitation, an account holder would presumably be able to share access with a third party so long as the third party's access was consistent with the computer's intended use.

d. The Ninth Circuit now applies the most restrictive definition of "authorized" access. The panel majority in this case concluded that a computer's owner "retain[s] exclusive discretion to issue or revoke access." Pet. App. 19a. And it approved an instruction to the jury that "[w]hether a person is authorized to access the computers in this case depends on the actions taken by [a computer's owner] to grant or deny permission to that person to use the computer." Pet. App. 24a. The Ninth Circuit

thus rejects the flexibility of the First, Fifth, and Seventh Circuits' approaches. At the same time, the Ninth Circuit's analysis turns on an examination of the owner's preferences, policies, and relationships—factors the Second and Fourth Circuits emphatically reject. Indeed, the panel majority suggested that whether access is "authorized" could depend on how "stark[ly]" the owner states its preferences and how "sympathetic" the access was, Pet. App. 19a—an argument indistinguishable from one the Second Circuit dismissed out of hand in *Valle*. 807 F.3d at 528; *see supra* p. 11.[2]

The split is entrenched and the grab-bag of approaches it subsumes undermines the statute's integrity and "fail[s] to provide fair notice to ordinary people who are required to conform their conduct to the law." *United States* v. *Kozminski*, 487 U.S. 931, 949-950 (1988). This Court's intervention is urgently needed.

II. THIS CASE IS A SUPERIOR VEHICLE TO ADDRESS THE QUESTION PRESENTED

The decision below was followed one day later by a ruling from a different panel of the Ninth Circuit, holding that Facebook had exclusive discretion to control access to its users' accounts even though they had consented to access by a third-party social media

---

[2] Although the panel majority recognized that *Nosal I* held that the CFAA does not punish "violations of corporate computer use restrictions or violations of a duty of loyalty," Pet. App. 15a (internal quotation marks omitted), it distinguished that decision on the ground that *Nosal I* addressed "unauthorized *use* of information" whereas "Nosal is [now] charged with unauthorized *access*." Pet. App. 16a (emphases added).

platform. *Facebook, Inc.* v. *Power Ventures, Inc.*, 844 F.3d 1058, 1067-68 (9th Cir. 2016).[3] The defendants in *Power Ventures* filed a petition for a writ of certiorari from this Court on March 9, 2017. *See Power Ventures, Inc.* v. *Facebook, Inc.*, No. 16-1105. The question presented by *Power Ventures* is closely related to the one presented by this case: both go to whether an account holder may confer "authorization" under the CFAA. *See* Pet. at 11-13, 23-26, *Power Ventures*, *supra* (No. 16-1105) (discussing the decision below). But this case is a better vehicle to address the question for three reasons.

First, the petitioners in *Power Ventures* do not contend that their case implicates the split described above. Instead, they base their argument largely on facts peculiar to the "novel" application of the CFAA to online social networks, which is "in stark contrast to prior CFAA private claimants—typically employers or former employers." Pet. at 9, 12, *Power Ventures*, *supra* (No. 16-1105); *cf id*. at 24 (explaining that this case *does* implicate a split). That points up a second reason to prefer this vehicle; the facts in this case are in the statute's heartland and easily analogized to the leading cases in the Circuits. Finally, this case involves an application of the Act's criminal sanctions, while *Power Ventures* is a private civil case. Resolving the question presented here in

---

[3] Because the defendants "could have thought that consent from *Facebook users* to" use their accounts "was permission for [the defendants] to access *Facebook's* computers," the *Power Ventures* court held that the defendants were liable only for accessing Facebook after the company issued a cease and desist letter "expressly rescinding" that "arguable permission." 844 F.3d at 1067.

the context of a criminal prosecution, where the stakes are highest, sharpens the issues and ensures consistent application of the statute across the criminal and civil contexts. *Cf. United States* v. *U.S. Gypsum Co.*, 438 U.S. 422, 438-439 (1978) (noting that interpreting the Sherman Act primarily as a civil statute had rendered its scope "indetermina[te]").

Nevertheless, if this Court grants review in *Power Ventures*, Mr. Nosal respectfully requests that the Court grant this petition and consolidate the cases for argument. *See, e.g.*, *Exxon Mobil Corp.* v. *Allapattah Servs., Inc.*, 545 U.S. 546, 549-550 (2005) (consolidating and jointly disposing of two distinct cases presenting the same question of statutory interpretation). At the very least, this Court should hold this petition pending resolution of the *Power Ventures* case.

III. THE QUESTION IS IMPORTANT AND RECURRING

The question presented has far-reaching implications. The CFAA covers anyone "who uses a computer, smartphone, iPad, Kindle, Nook, X-box, Blu-Ray player or any other Internet-enabled device." *Nosal I*, 676 F.3d at 861. Every time a user loads a web page, checks his email, or logs into a social media account, he accesses computers owned or controlled by the publishers or providers of those services. *See id.* If the Ninth Circuit's decision is allowed to stand, whether that access is "authorized" or whether it is instead a federal crime will depend on "a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands"—precisely the result the Ninth Circuit

itself sought to avoid when it construed the statute's bar on exceeding authorized access in *Nosal I*. *Id*.

Password-protected user accounts are a ubiquitous means of controlling access to a vast array of online services. Often, these accounts exist as a way for companies to gain valuable marketing data. In other cases, account-based access protects *user* information such as emails, documents, or digital photographs. The use of these accounts is governed by private agreements, many of which expressly forbid password-sharing or impose other categorical prohibitions on who may access the website's services.[4]

The panel majority below insisted that "[t]his appeal is not about password sharing. Nor is it about violating a company's internal computer-use policies." Pet. App. 5a. And it paid lip service to *Nosal I*'s holding that "violating use restrictions * * * is insufficient without more to form the basis for liability under the CFAA." Pet. App. 23a. But that is not consistent with a fair reading of the decision below, as the dissent explained. The majority held that a computer's owner "retain[s] exclusive discretion to issue or revoke" authorization within the meaning of

---

[4] *See, e.g.*, Facebook Statement of Rights and Responsibilities, effective January 30, 2015 ("You will not share your password * * * [or] let anyone else access your account * * * ."), *available at* https://www.facebook.com/legal/terms (last visited May 4, 2017); New York Times Terms of Service (effective November 17, 2015) ("You are not allowed to share your registration login credentials or give your login credentials to anyone else."), *available at* https://www.nytimes.com/content/help/rights/terms/terms-of-service.html (last visited May 4, 2017); Twitter Terms of Service, effective September 30, 2016 ("[Y]ou must be at least 13 years old to use the Services."), *available at* https://twitter.com/tos?lang=en (last visited May 4, 2017).

the Act. *Id.* at 19a. It thus affirmed a jury verdict based on an instruction that expressly defined "authorization" as permission from the computer's owner. *Id.* at 24a-25a. The inescapable import of the panel's holding is that accessing a computer in contravention of a use policy is a federal crime. *See Id.* at 60a-61a (Reinhardt, J., dissenting). After all, a policy that expressly bars sharing an account password, or that prohibits anyone under the age of 13 from opening an account can hardly be said to "grant * * * permission" to do those things. *Id.* at 18a (majority opinion); *see supra* n.4. And the panel explained that an account holder "ha[s] no mantle or authority to override [the owner's] authority to control access to its computers." Pet. App. 18a.

As the dissent and amici below explained, the panel majority's rule makes a crime out of such innocuous activities as "an office worker asking a friend to log into his email in order to print a boarding pass, in violation of the system owner's access policy; or * * * one spouse asking the other to log into a bank website to pay a bill, in violation of the bank's password sharing prohibition." Pet. App. 54a (Reinhardt, J., dissenting). It does the same for a husband who logs into his wife's Facebook account with her permission. *See* EFF *Amicus* Br. 17-18, *United States* v. *Nosal* (9th Cir. No. 14-10037), Doc. 14.[5]

[5] The decision below and the confusion among the Circuits have also attracted extensive academic commentary, including a recent symposium hosted by the George Washington Law Review devoted to the CFAA. *See* Symposium, *Hacking Into the Computer Fraud and Abuse Act: The CFAA at 30*, 84 G.W. L. Rev. 1437 (2016).

The very nature of networked computing compounds the problem: A person who logs into their Facebook account on a work computer is accessing both the employer's computer *and* Facebook's computers—not to mention the untold numbers of third-party computers that make the Internet possible. Under the majority's rule, a person who picks up his spouse's work-issued laptop and looks at her Facebook account has violated the CFAA *twice*—once by accessing the work-issued laptop without permission from his spouse's employer, and once by using a borrowed password to access Facebook's computers.

The majority's rule has broader social implications, too. It threatens to chill research carried out by journalists and scholars to uncover online discrimination and other abuses. *See* EFF & ACLU *Amicus* Br. in Support of Reh'g En Banc 15-18, *Nosal*, *supra*, Doc. 73. Audit testing has long been a valuable tool for ferreting out violations of civil rights laws. *See Havens Realty Corp.* v. *Coleman*, 455 U.S. 363, 373 (1982). The online equivalent of such testing may require accessing members' accounts with their permission or creating test accounts to see how users with different demographic profiles are treated. Under the majority's rule, a company need only prohibit such research in its terms of service to transform an essential means of enforcing the law into a crime itself.

Finally, the panel majority's anachronistic view of computer use threatens unintended consequences for the increasing trend towards so-called "cloud" computing. *See generally* BSA|The Software Alliance *Amicus* Br., *Nosal*, *supra*, Doc. 17. Computing services are increasingly provided online through remote servers referred to as the "cloud." *Id.* These

services permit users to store data and even use applications that are hosted remotely on hardware owned by the service provider. Remote hosting offers lower costs, better security, and enhanced flexibility. But it also departs from the traditional model of computing in which a user uses applications or data stored on a single machine or a local server. Instead, the account holder's work is both performed and stored on the service's computers. In such circumstances, sharing a password or account is not functionally different from choosing to share one's personal computer. But if the decision below stands, it is a federal crime without permission from the cloud service provider.

The panel majority claimed that such concerns "can be reserved for another day." Pet. App. 19a-20a. They cannot. The decision below creates a per se rule that applies throughout the Ninth Circuit: Access without permission from a computer's owner is access "without authorization" under the CFAA. This Court's review is needed now.

IV. THE NINTH CIRCUIT'S DECISION WAS INCORRECT

The panel majority thought that the CFAA "unambiguous[ly]" forbids accessing a computer without the owner's permission. Pet. App. 18a-20a, 24a. It does not. In fact, the statute says nothing whatsoever about *who* may authorize access to a computer. In light of the CFAA's text, purpose, and the rule of lenity, the better reading is that *either* the owner or an account holder can authorize access and that they must grant or revoke authorization unequivocally by establishing or removing technological access barriers.

1. The CFAA does not define "without authorization." *See* Pet. App. 12a. The meaning of that term "has proven to be elusive." *EF Cultural Travel*, 274 F.3d at 582 n.10. The panel majority, however, believed that "without authorization" is "unambiguous" because the word "authorization" is commonly defined as "permission." Pet. App. 17a-18a. Relying on this "straightforward meaning," it concluded that only a computer's owner—in this case, Korn/Ferry—could "authorize" access and that an account holder "had no mantle or authority" to do so on her own. Pet. App. 18a. That was quite a leap. Observing that "without authorization" means "without permission" does not even suggest, let alone establish unambiguously, that permission may come only from a computer's owner. Yet that was the extent of the panel majority's analysis of the central question in this case.

The Government did not dispute that Nosal's former assistant voluntarily shared her valid login credentials with his colleagues. *See, e.g.*, U.S. Br. 16-17, 20, *Nosal*, *supra*, Doc. 28-1. If they accessed Korn/Ferry's computers, they did so literally with "permission." Mr. Nosal's innocence or guilt of the password-sharing counts thus turns on whether that permission is sufficient under the CFAA.

From the face of the statute, there is no more reason to think that "without authorization" means "without the owner's permission" than there is to think it means "without an account holder's permission." Read in light of the statute's anti-hacking purpose, the most sensible conclusion is that *both* an owner and an account holder are valid sources of permission. That construction is not merely "possible to articulate," as the panel majority dismissively

suggested. Pet. App. 18a n.6 (quoting *Moskal* v. *United States*, 498 U.S. 103, 108 (1990)). It is consistent with the statutory text. *See United States* v. *Santos*, 553 U.S. 507, 513-514 (2008) (finding ambiguity where "all provisions of the *** statute are coherent; no provisions are redundant; and the statute is not rendered utterly absurd" under either of two possible interpretations). And it comports with Congress's stated intention to deter hackers from "breaking and entering" into computers. H.R. Rep. 98-894, at 20; *see* H.R. Rep. 99-612, at 5-6. By contrast, interpreting the CFAA to require an owner's permission risks "criminaliz[ing] a broad range of day-to-day activity"—a result Congress is highly unlikely to have intended. *Kozminski*, 487 U.S. at 949; *see supra* pp. 19-21.

The rule of lenity has particular bite where the broader reading of a statute threatens to turn every computer user in the country into an unwitting federal criminal. This Court has long required that Congress speak "in language that is clear and definite" before it will "choose the harsher" of two possible readings of a criminal statute. *Jones* v. *United States*, 529 U.S. 848, 858 (2000) (internal quotation marks omitted). Any "doubts are resolved in favor of the defendant." *United States* v. *Bass*, 404 U.S. 336, 348 (1971); *see Santos*, 553 U.S. at 514 ("Under a long line of our decisions, the tie must go to the defendant."). Under that rule, the Ninth Circuit was "bound to adopt the construction of [the] CFAA that criminalizes access only by those without permission from *either* an account holder *or* the system owner," Pet. App. 58a-59a (Reinhardt, J., dissenting), and to vacate Mr. Nosal's convictions.

None of this is to say that individuals who access computers for tortious or criminal purposes must go unpunished. Other state and federal laws provide ample civil remedies and grounds for criminal prosecution of wrongdoers. *See, e.g.*, *WEC Carolina*, 687 F.3d at 207 & n.4 (declining to adopt a broad construction of the CFAA "given that other legal remedies exist for these grievances"). The CFAA addresses one particular concern: hacking. Vindicating that purpose does not require adopting the Ninth Circuit's reading of the statute.

2. The panel majority also erred in rejecting Mr. Nosal's challenge to the jury instruction that "[w]hether a person is authorized to access the computers * * * depends on the actions taken by [the owner] to grant or deny permission to that person to use the computer." Pet. App. 24a.

If that instruction were correct, "the statute[] would provide almost no objective indication of the conduct or condition [it] prohibit[s]." *Kozminski*, 487 U.S. at 949-950. Whether access was illegal would depend instead on *private* contracts, policies, or communications. *See supra* pp. 17-19. And that "would fail to provide fair notice to ordinary people who are required to conform their conduct to the law." *Kozminski*, 487 U.S. at 949-950.

These concerns are best addressed by construing "authorization" in light of the CFAA's anti-hacking purpose. Hacking, as the Ninth Circuit explained in *Nosal I*, is "the circumvention of technological access barriers." 676 F.3d at 863. The panel majority thought the evidence in this case met that test because "[t]he password system adopted by Korn/Ferry is unquestionably a technological barri-

er." Pet. App. 26a. But the majority's conclusion does not follow from its premise. Real circumvention might involve technological attacks, such as computer programs designed to guess at thousands of possible passwords. *See Phillips*, 477 F.3d at 217 n.1, 220. Or it could involve obtaining legitimate credentials through fraud, such as "phishing." Indeed, the statute specifically prohibits "traffic[king] * * * in any password or similar information through which a computer may be accessed without authorization." 18 U.S.C. § 1030(a)(6). But a person who gains admission to a computer with a legitimately borrowed password does not "circumvent" a password system any more than a houseguest who uses his host's key "circumvents" a lock.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

THOMAS P. SCHMIDT
HOGAN LOVELLS US LLP
875 Third Avenue
New York, NY 10022

DENNIS P. RIORDAN
TED SAMPSELL-JONES
RIORDAN & HORGAN
523 Octavia Street
San Francisco, CA 94102

NEAL KUMAR KATYAL
Counsel of Record
EUGENE A. SOKOLOFF
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5600
neal.katyal@hoganlovells.com

Counsel for Petitioner

May 2017

APPENDIX

APPENDIX A

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Nos. 14-10037, 14, 10275

D.C. No. 3:08-cr-00237-EMC-1

UNITED STATES OF AMERICA
Plaintiff-Appellee,

v.

DAVID NOSAL,
Defendant-Appellant.

Appeals from the United States District Court
for the Northern District of California

Argued and Submitted October 2, 2015

Filed July 5, 2016
Amended December 8, 2016

Before: THOMAS, Chief Judge, and REINHARDT and McKEOWN, Circuit Judges.

ORDER

The opinion filed on July 5, 2016, and appearing at 828 F.3d 865, is hereby amended. An amended opinion is filed concurrently with this order.

With these amendments, Chief Judge Thomas and Judge McKeown vote to deny the petition for rehearing en banc. Judge Reinhardt votes to grant the petition for rehearing en banc.

The full court has been advised of the petition for rehearing en banc, and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for rehearing en banc is denied. No further petitions for en banc or panel rehearing shall be permitted.

OPINION

McKEOWN, Circuit Judge:

This is the second time we consider the scope of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, with respect to David Nosal. The CFAA imposes criminal penalties on 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." *Id.* § 1030(a)(4) (emphasis added).

Only the first prong of the section is before us in this appeal: "knowingly and with intent to defraud" accessing a computer "without authorization." Embracing our earlier precedent and joining our sister circuits, we conclude that "without authorization" is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission. Further, we have held that authorization is not pegged to website terms and

conditions. This definition has a simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party. Unequivocal revocation of computer access closes both the front door and the back door. This provision, coupled with the requirement that access be "knowingly and with intent to defraud," means that the statute will not sweep in innocent conduct, such as family password sharing.

Nosal worked at the executive search firm Korn/Ferry International when he decided to launch a competitor along with a group of co-workers. Before leaving Korn/Ferry, Nosal's colleagues began downloading confidential information from a Korn/Ferry database to use at their new enterprise. Although they were authorized to access the database as current Korn/Ferry employees, their downloads on behalf of Nosal violated Korn/Ferry's confidentiality and computer use policies. In 2012, we addressed whether those employees "exceed[ed] authorized access" with intent to defraud under the CFAA. *United States* v. *Nosal* (*Nosal I*), 676 F.3d 854 (9th Cir. 2012) (en banc). Distinguishing between access restrictions and use restrictions, we concluded that the "exceeds authorized access" prong of § 1030(a)(4) of the CFAA "does not extend to violations of [a company's] use restrictions." *Id.* at 863. We affirmed the district court's dismissal of the five CFAA counts related to Nosal's aiding and abetting misuse of data accessed by his co-workers with their own passwords.

The remaining counts relate to statutory provisions that were not at issue in *Nosal I*: access to a protected computer "without authorization" under the CFAA and trade secret theft under the Economic Espionage Act ("EEA"), 18 U.S.C. § 1831 *et seq*. When Nosal left Korn/Ferry, the company revoked his computer access credentials, even though he remained for a time as a contractor. The company took the same precaution upon the departure of his accomplices, Becky Christian and Mark Jacobson. Nonetheless, they continued to access the database using the credentials of Nosal's former executive assistant, Jacqueline Froehlich-L'Heureaux ("FH"), who remained at Korn/Ferry at Nosal's request. The question we consider is whether the jury properly convicted Nosal of conspiracy to violate the "without authorization" provision of the CFAA for unauthorized access to, and downloads from, his former employer's database called Searcher.[1] Put simply, we are asked to decide whether the "without authorization" prohibition of the CFAA extends to a former employee whose computer access credentials have been rescinded but who, disregarding the revocation, accesses the computer by other means.

We directly answered this question in *LVRC Holdings LLC* v. *Brekka*, 581 F.3d 1127 (9th Cir. 2009), and reiterate our holding here: "[A] person

[1] As in *Nosal I*, Nosal did not himself access and download information from Korn/Ferry's database. Nosal was convicted of three substantive CFAA counts on either an aiding and abetting or conspiracy theory. Under either, Nosal is liable for the conduct of Christian and Jacobson. *See Pinkerton* v. *United States*, 328 U.S. 640, 647 (1946) (conspiracy liability); *United States* v. *Short*, 493 F.2d 1170, 1172 (9th Cir. 1974) (aiding and abetting liability).

uses a computer 'without authorization' under [the CFAA] *** when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id.* at 1135. This straightforward principle embodies the common sense, ordinary meaning of the "without authorization" prohibition.

Nosal and various amici spin hypotheticals about the dire consequences of criminalizing password sharing. But these warnings miss the mark in this case. This appeal is not about password sharing. Nor is it about violating a company's internal computer-use policies. The conduct at issue is that of Nosal and his co-conspirators, which is covered by the plain language of the statute. Nosal is charged with conspiring with former Korn/Ferry employees whose user accounts had been terminated, but who nonetheless accessed trade secrets in a proprietary database through the back door when the front door had been firmly closed. Nosal knowingly and with intent to defraud Korn/Ferry blatantly circumvented the affirmative revocation of his computer system access. This access falls squarely within the CFAA's prohibition on "knowingly and with intent to defraud" accessing a computer "without authorization," and thus we affirm Nosal's conviction for violations of § 1030(a)(4) of the CFAA.

The dissent mistakenly focuses on FH's authority, sidestepping the authorization question for Christian and Jacobson. To begin, FH had no authority from Korn/Ferry to provide her password to former employees whose computer access had been revoked. Also, in collapsing the distinction between FH's authorization and that of Christian and Jacobson,

the dissent would render meaningless the concept of authorization. And, pertinent here, it would remove from the scope of the CFAA any hacking conspiracy with an inside person. That surely was not Congress's intent.

We also affirm Nosal's convictions under the EEA for downloading, receiving and possessing trade secrets in the form of source lists from Searcher. We vacate in part and remand the restitution order for reconsideration of the reasonableness of the attorneys' fees award.

BACKGROUND

I. FACTUAL BACKGROUND

Nosal was a high-level regional director at the global executive search firm Korn/Ferry International. Korn/Ferry's bread and butter was identifying and recommending potential candidates for corporate positions. In 2004, after being passed over for a promotion, Nosal announced his intention to leave Korn/Ferry. Negotiations ensued and Nosal agreed to stay on for an additional year as a contractor to finish a handful of open searches, subject to a blanket non-competition agreement. As he put it, Korn/Ferry was giving him "a lot of money" to "stay out of the market."

During this interim period, Nosal was very busy, secretly launching his own search firm along with other Korn/Ferry employees, including Christian, Jacobson and FH. As of December 8, 2004, Korn/Ferry revoked Nosal's access to its computers, although it permitted him to ask Korn/Ferry employees for research help on his remaining open

assignments. In January 2005, Christian left Korn/Ferry and, under instructions from Nosal, set up an executive search firm—Christian & Associates—from which Nosal retained 80% of fees. Jacobson followed her a few months later. As Nosal, Christian and Jacobson began work for clients, Nosal used the name "David Nelson" to mask his identity when interviewing candidates.

The start-up company was missing Korn/Ferry's core asset: "Searcher," an internal database of information on over one million executives, including contact information, employment history, salaries, biographies and resumes, all compiled since 1995. Searcher was central to Korn/Ferry's work for clients. When launching a new search to fill an open executive position, Korn/Ferry teams started by compiling a "source list" of potential candidates. In constructing the list, the employees would run queries in Searcher to generate a list of candidates. To speed up the process, employees could look at old source lists in Searcher to see how a search for a similar position was constructed, or to identify suitable candidates. The resulting source list could include hundreds of names, but then was narrowed to a short list of candidates presented to the client. Korn/Ferry considered these source lists proprietary.

Searcher included data from a number of public and quasi-public sources like LinkedIn, corporate filings and Internet searches, and also included internal, non-public sources, such as personal connections, unsolicited resumes sent to Korn/Ferry and data inputted directly by candidates via Korn/Ferry's website. The data was coded upon entry; as a result, employees could run targeted

searches for candidates by criteria such as age, industry, experience or other data points. However, once the information became part of the Searcher system, it was integrated with other data and there was no way to identify the source of the data.

Searcher was hosted on the company's internal computer network and was considered confidential and for use only in Korn/Ferry business. Korn/Ferry issued each employee a unique username and password to its computer system; no separate password was required to access Searcher. Password sharing was prohibited by a confidentiality agreement that Korn/Ferry required each new employee to sign. When a user requested a custom report in Searcher, Searcher displayed a message which stated: "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only."

Nosal and his compatriots downloaded information and source lists from Searcher in preparation to launch the new competitor. Before leaving Korn/Ferry, they used their own usernames and passwords, compiling proprietary Korn/Ferry data in violation of Korn/Ferry's computer use policy. Those efforts were encompassed in the CFAA accounts appealed in *Nosal I*. *See* 676 F.3d at 856.

After Nosal became a contractor and Christian and Jacobson left Korn/Ferry, Korn/Ferry revoked each of their credentials to access Korn/Ferry's computer system. Not to be deterred, on three occasions Christian and Jacobson borrowed access credentials from FH, who stayed on at Korn/Ferry at Nosal's request. In April 2005, Nosal instructed Christian to

obtain some source lists from Searcher to expedite their work for a new client. Thinking it would be difficult to explain the request to FH, Christian asked to borrow FH's access credentials, which Christian then used to log in to Korn/Ferry's computer system and run queries in Searcher. Christian sent the results of her searches to Nosal. In July 2005, Christian again logged in as FH to generate a custom report and search for information on three individuals. Later in July, Jacobson also logged in as FH, to download information on 2,400 executives. None of these searches related to any open searches that fell under Nosal's independent contractor agreement.

In March 2005, Korn/Ferry received an email from an unidentified person advising that Nosal was conducting his own business in violation of his non-compete agreement. The company launched an investigation and, in July 2005, contacted government authorities.

II. PROCEDURAL BACKGROUND

In the first indictment, Nosal was charged with twenty criminal counts, including eight counts under the CFAA, two trade secrets counts under the Economic Espionage Act and one conspiracy count. Five of the eight CFAA counts were based on allegations that FH and Christian downloaded material from Searcher using their own credentials while employed by Korn/Ferry in violation of company policies. The district court dismissed these counts, citing our decision in *Brekka*, 581 F.3d 1127. That dismissal was affirmed by the en banc court in

Nosal I, and the case was remanded for trial on the remaining counts. 676 F.3d at 864.

The government filed a second superseding indictment in February 2013 with three CFAA counts, two trade secrets counts and one conspiracy count. Nosal's remaining CFAA counts were based on the three occasions when Christian and Jacobson accessed Korn/Ferry's system for their new clients using FH's login credentials. The district court denied Nosal's motion to dismiss the three remaining CFAA counts, rejecting the argument that *Nosal I* limited the statute's applicability "to hacking crimes where the defendant circumvented technological barriers to access a computer." *United States* v. *Nosal*, 930 F. Supp. 2d 1051, 1060 (N.D. Cal. 2013). Alternatively, the court held that "the indictment sufficiently allege[d] such circumvention." *Id*. at 1061. A jury convicted Nosal on all counts. The district court sentenced Nosal to one year and one day in prison, three years of supervised release, a $60,000 fine, a $600 special assessment and approximately $828,000 in restitution to Korn/Ferry.

ANALYSIS

I. CONVICTIONS UNDER THE COMPUTER FRAUD AND ABUSE ACT

A. Background of the CFAA

The CFAA was originally enacted in 1984 as the Counterfeit Access Device and Computer Fraud and Abuse Act, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190 (1984). The act was aimed at "hackers who accessed computers to steal information or to disrupt or destroy computer functionality." *Brekka*, 581 F.3d

at 1130-31 (citing H.R. Rep. No. 98-894, at 8-9 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694). The original legislation protected government and financial institution computers,[2] and made it a felony to access classified information in a computer "without authorization." Counterfeit Access Device and Computer Fraud and Abuse Act § 2102(a).

Just two years later in 1986, Congress amended the statute to "deter[] and punish[] certain 'high-tech' crimes," and "to penalize thefts of property via computer that occur as part of a scheme to defraud," S. Rep. No. 99-432, at 4, 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482, 2486-87. The amendment expanded the CFAA's protections to private computers. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(g)(4), 100 Stat. 1213-15.[3]

The key section of the CFAA at issue is 18 U.S.C. § 1030(a)(4), which provides in relevant part:

---

[2] A computer is defined broadly as "an electronic * * * data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1). The CFAA's restrictions have been applied to computer networks, databases and cell phones. *See, e.g., United States* v. *Valle*, 807 F.3d 508, 513 (2d Cir. 2015) (restricted police databases); *United States* v. *Barrington*, 648 F.3d 1178, 1184 (11th Cir. 2011) (a university's Internet-based grading system); *United States* v. *Kramer*, 631 F.3d 900, 903 (8th Cir. 2011) (cell phones); *United States* v. *Shea*, 493 F.3d 1110, 1115-16 (9th Cir. 2007) (computer network).

[3] The act was later expanded to protect any computer "used in interstate or foreign commerce or communication." Economic Espionage Act of 1996, Pub. L. 104-294, § 201(4)(B), 110 Stat. 3488, 3493 (codified as amended at 18 U.S.C. § 1030(e)(2)(B)).

> 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 * * * shall be punished * * * .

A key element of the statute is the requirement that the access be "knowingly and with intent to defraud." Not surprisingly, this phrase is not defined in the CFAA as it is the bread and butter of many criminal statutes. Indeed, the district court borrowed the language from the Ninth Circuit model jury instructions in defining "knowingly" and "intent to defraud" for the jury, and Nosal does not renew any challenges to those instructions on appeal. This mens rea element of the statute is critical because imposing the "intent to defraud" element targets knowing and specific conduct and does not embrace the parade of hypotheticals generated by Nosal and amici.

The CFAA defines "exceeds authorized access" as "access [to] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6). The statute does not, however, define "without authorization." Both terms are used throughout § 1030. Subsection 1030(a)(2), which mirrors (a)(4) but requires that access be intentional, penalizes access without authorization and exceeding authorization. Subsection 1030(a)(1) also incorporates both terms in relation to accessing a computer and obtaining national security information. Subsection 1030(a)(7)(B) criminalizes extortion by threats to

obtain information "without authorization or in excess of authorization." The remaining subsections pertain only to access "without authorization." Subsection 1030(a)(3) prohibits access "without authorization" to nonpublic government computers. Subsections 1030(a)(5) and (6) employ the term "without authorization" with respect to, among other things, "transmission of a program, information, code, or command," § 1030(a)(5)(A); intentional access that "causes damage and loss," § 1030(a)(5)(C); and trafficking in passwords, § 1030(a)(6). In construing the statute, we are cognizant of the need for congruence among these subsections.

B. Meaning of "Authorization" Under the CFAA

The interpretive fireworks under § 1030(a)(4) of the CFAA have been reserved for its second prong, the meaning of "exceeds authorized access." Not surprisingly, there has been no division among the circuits on the straightforward "without authorization" prong of this section. We begin with the two Ninth Circuit cases that bind our interpretation of "without authorization"—*Brekka* and *Nosal I*—and then move on to address the cases from our sister circuits that are in accord with *Brekka*, agreeing that "without authorization" is an unambiguous term that should be given its ordinary meaning.

Brekka involved a former employee in circumstances remarkably similar to Nosal: he wanted to compete using confidential data from his former company. Christopher Brekka worked as an

internet marketer with LVRC Holdings, LLC ("LVRC"), a residential addiction treatment center. *Brekka*, 581 F.3d at 1129. LVRC assigned him a computer and gave him access credentials to a third-party website that tracked traffic and other information for LVRC's website. *Id.* at 1129-30. When negotiations to become part owner of LVRC broke down, Brekka left the company. *Id.* at 1130. LVRC sued him, claiming that he violated the CFAA by emailing certain confidential company documents to his personal email account while an employee and also by continuing to access LVRC's account on the external website after he left the company. *Id.*

In *Brekka* we analyzed both the "without authorization" and "exceeds authorization" provisions of the statute under §§ 1030(a)(2) and (4). *Id.* at 1132-36. Because the CFAA does not define the term "authorization," we looked to the ordinary, contemporaneous meaning of the term: "'permission or power granted by an authority.'" *Id.* at 1133 (quoting Random House Unabridged Dictionary 139 (2001)). In determining whether an employee has authorization, we stated that, consistent with "the plain language of the statute * * * 'authorization' [to use an employer's computer] depends on actions taken by the employer." *Id.* at 1135. We concluded that because Brekka had permission to use his employer's computer, "[t]he most straightforward interpretation of §§ 1030(a)(2) and (4) is that Brekka had authorization to use the computer" while an employee. *Id.* at 1133.

Brekka's access after LVRC terminated his employment presented a starkly different situation: "There is no dispute that if Brekka accessed LVRC's

information on the [traffic monitoring] website after he left the company * * *, Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA." *Id.* at 1136.[4] Stated differently, we held that "a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) * * * when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id.* at 1135. In Brekka's case, there was no genuine issue of material fact as to whether Brekka actually accessed the website, and thus we affirmed the district court's grant of summary judgment. *Id.* at 1137.

Not surprisingly, in *Nosal I* as in this appeal, both the government and Nosal cited *Brekka* extensively. The focus of Nosal's first appeal was whether the CFAA could be interpreted "broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty." *Nosal I*, 676 F.3d at 862. We unequivocally said "no": "For our part, we continue to follow in the path blazed by *Brekka* and the growing number of courts that have reached the same conclusion. These courts recognize that the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'" *Id.* at 863 (citations omitted) (alteration in original). In

[4] Brekka's authorization terminated when his employment terminated, not because his password expired. Expired passwords do not necessarily mean that authorization terminates: authorized account-holders often let their passwords lapse before updating the password or contacting the company's technical support team for help, but expiration of a password doesn't necessarily mean that account authorization has terminated.

line with *Brekka*, we stated that "'[w]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorization access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." *Id.* at 858 (emphases in original). Because Nosal's accomplices had authority to access the company computers, we affirmed the district court's dismissal of the CFAA counts related to the period when the accomplices were still employed at Korn/Ferry. *Id.* at 864.

In *Nosal I*, authorization was not in doubt. The employees who accessed the Korn/Ferry computers unquestionably had authorization from the company to access the system; the question was whether they exceeded it. What *Nosal I* did not address was whether Nosal's access to Korn/Ferry computers *after* both Nosal and his coconspirators had terminated their employment and Korn/Ferry revoked their permission to access the computers was "without authorization." *Brekka* is squarely on point on that issue: Nosal and his co-conspirators acted "without authorization" when they continued to access Searcher by other means after Korn/Ferry rescinded permission to access its computer system. As *Nosal I* made clear, the CFAA was not intended to cover unauthorized use of information. Such *use* is not at issue here. Rather, under § 1030(a)(4), Nosal is charged with unauthorized access—getting into the computer after categorically being barred from entry.

The text of the CFAA confirms *Brekka*'s approach. Employing classic statutory interpretation, we

consider the plain and ordinary meaning of the words "without authorization." *See United States* v. *Stewart*, 311 U.S. 60, 63 (1940). Under our analysis in *Brekka*, "authorization" means "'permission or power granted by an authority.'" 581 F.3d at 1133 (quoting Random House Unabridged Dictionary 139 (2001)). Other sources employ similar definitions. Black's Law Dictionary defines "authorization" as "[o]fficial permission to do something; sanction or warrant." *Black's Law Dictionary* 159 (10th ed. 2014). The Oxford English Dictionary defines it as "the action of authorizing," which means to "give official permission for or approval to." *Oxford English Dictionary* 107 (3d ed. 2014). That common sense meaning is not foreign to Congress or the courts: the terms "authorize," "authorized" or "authorization" are used without definition over 400 times in Title 18 of the United States Code.[5] We conclude that given its ordinary meaning, access "without authorization" under the CFAA is not ambiguous. *See United States* v. *James*, 810 F.3d 674, 681 (9th Cir. 2016) (concluding that the mere

[5] For example, Title 18 covers a number of offenses that stem from conduct "without authorization." *See, e.g.*, 18 U.S.C. § 1388(a)(2)(B) (holding liable any person who "willfully and without proper authorization imped[es]" access to a funeral of a member of the Armed Forces); 18 U.S.C. § 1831(a) (holding liable for economic espionage "[w]hoever, intending or knowing that the offense will benefit any foreign government * * * knowingly * * * without authorization appropriates, takes, carries away, or conceals" trade secrets); 18 U.S.C. § 2701 (holding liable any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided * * * and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage").

fact that a broad, but otherwise clear, statutory term is "susceptible to application to various factual situations that can come before a jury" does not by itself render a term ambiguous).

That straightforward meaning is also unambiguous as applied to the facts of this case.[6] Nosal and his co-conspirators did exactly what *Brekka* prohibits—a conclusion that is not affected by the co-conspirators' use of FH's legitimate access credentials. Implicit in the definition of authorization is the notion that someone, including an entity, can grant or revoke that permission. Here, that entity was Korn/Ferry, and FH had no mantle or authority to override Korn/Ferry's authority to control access to its computers and confidential information by giving permission to former employees whose access had been categorically revoked by the company. [7]

---

[6] We do not invoke the rule of lenity because "the touchstone of the rule of lenity is statutory ambiguity," *Bifulco* v. *United States*, 447 U.S. 381, 387 (1980) (internal quotation marks omitted), and "[t]he rule comes into operation at the end of the process of construing what Congress has expressed, not at the beginning as an overriding consideration of being lenient to wrongdoers," *Callanan* v. *United States*, 364 U.S. 587, 596 (1961). Here, because the statute "unambiguously cover[s] the defendant's conduct, the rule does not come into play." *United States* v. *Litchfield*, 986 F.2d 21, 22 (2d Cir. 1993). That the CFAA might support a narrower interpretation, as the dissent argues, does not change our analysis. *See Moskal* v. *United States*, 498 U.S. 103, 108 (1990) (holding that the rule of lenity is not triggered because it is "possible to articulate" a narrower construction of a statute).

[7] The dissent rests its argument on the fact that Brekka had "no possible source of authorization." The same is true here—Nosal had "no possible source of authorization" since the company revoked his authorization and, while FH might have

Korn/Ferry owned and controlled access to its computers, including the Searcher database, and it retained exclusive discretion to issue or revoke access to the database. By revoking Nosal's login credentials on December 8, 2004, Korn/Ferry unequivocally conveyed to Nosal that he was an "outsider" who was no longer authorized to access Korn/Ferry computers and confidential information, including Searcher.[8] Korn/Ferry also rescinded Christian and Jacobson's credentials after they left, at which point the three former employees were no longer "insiders" accessing company information. Rather, they had become "outsiders" with no authorization to access Korn/Ferry's computer system.[9] One can certainly pose hypotheticals in which a less stark revocation is followed by more sympathetic access through an authorized third party. But the facts before us—in which Nosal received particularized notice of his revoked access

---

been wrangled into giving out her password, she and the others knew that she had no authority to control system access.

[8] Nosal argues that he cannot be held liable because, as a contractor, he was entitled to access information from Korn/Ferry's database. Nosal misconstrues his authorization following his departure from Korn/Ferry: he was entitled only to information related to his open searches, and being entitled to receive information does not equate to permission to access the database. Further, Nosal's liability as a co-conspirator turns on whether Christian and Jacobson acted "without authorization."

[9] We note that the terms "insider" and "outsider" in these circumstances are simply descriptive proxies for the status of the parties here and in *Brekka*. There obviously could be an "insider" in a company, such as a cleaning or maintenance person, who is not authorized to access any computer or company information but who, nonetheless, accesses the company computer "without authorization."

following a prolonged negotiation—present no such difficulties, which can be reserved for another day.

Our analysis is consistent with that of our sister circuits, which have also determined that the term "without authorization" is unambiguous.[10] Although the meaning of "exceeds authorized access" in the CFAA has been subject to much debate among the federal courts, [11] the definition of "without

---

[10] Although the Supreme Court recently affirmed a conviction under the CFAA with facts similar to those here, it did not address interpretation of "without authorization." *See Musacchio* v. *United States*, 136 S. Ct. 709 (2016). Without elaboration, the Court noted that "[t]he statute thus provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Id.* at 713.

[11] See discussion in *Nosal I*, 676 F.3d at 862-63. *Compare United States* v. *Valle*, 807 F.3d 508, 526-28 (2d Cir. 2015) (holding that while there is support for both a narrow and broad reading of "exceeds authorized access," the rule of lenity requires the court to adopt a narrower interpretation in the defendant's favor), *with WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (concluding that "an employee 'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access"), *and United States* v. *John*, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."), *and United States* v. *Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that an employee who violates employer use restrictions "exceeds authorized access"), *and Int'l Airport Ctrs., L.L.C.* v. *Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (holding that while the "difference between access 'without authorization' and 'exceeding authorized access' is paper thin," an employee who breached a duty of loyalty terminated the agency relationship and exceeded authorized access in using company laptop), *and*

authorization" has not engendered dispute. Indeed, Nosal provides no contrary authority that a former employee whose computer access has been revoked can access his former employer's computer system and be deemed to act with authorization.

Beginning in 1991, in construing § 1030(a)(5)(A),[12] the Second Circuit recognized that "authorization" is a word "of common usage, without any technical or ambiguous meaning." *United States* v. *Morris*, 928 F.2d 504, 511 (2d Cir. 1991). The court reaffirmed this holding in 2015, citing *Brekka* and stating that "common usage of 'authorization' suggests that one 'accesses a computer without authorization' if he accesses a computer without permission to do so at all." *United States* v. *Valle*, 807 F.3d 508, 524 (2d Cir. 2015).

The Fourth Circuit's analysis mirrors the conclusion that the "without authorization" language is unambiguous based on its ordinary meaning:

> Recognizing that the distinction between ["exceeds authorized access" and access "without authorization"] is arguably minute, we nevertheless conclude based on the ordinary, contemporary, common meaning of "authorization," that an employee is authorized to access a computer when his employer approves or sanctions his admission

---

EF Cultural Travel BV v. *Explorica, Inc.*, 274 F.3d 577, 581-84 (1st Cir. 2001) (holding that former employees who violated confidentiality agreements exceeded authorized access).

[12] This section of the CFAA criminalizes intentional "transmission of a program, information, code, or command" to a protected computer "without authorization" causing damage. 18 U.S.C. § 1030(a)(5)(A).

> to that computer. Thus, he accesses a computer "without authorization" when he gains admission to a computer without approval. Similarly, we conclude that an employee "exceeds authorized access" when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access.

WEC Carolina Energy Solutions LLC v. *Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (internal citations omitted).

Like the other courts, the Sixth Circuit noted that "[t]he plain meaning of 'authorization' is '[t]he conferment of legality; * * * sanction.' Commonly understood, then, a defendant who accesses a computer 'without authorization' does so without sanction or permission." *Pulte Homes, Inc.* v. *Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 303-04 (6th Cir. 2011) (quoting 1 *Oxford English Dictionary* 798 (2d ed. 1989)). Based on ordinary usage, the Sixth Circuit similarly reasoned that "'a person who uses a computer 'without authorization' *has no rights*, *limited or otherwise*, to access the computer in question.'" *Id.* at 304 (alteration in original) (quoting *Brekka*, 581 F.3d at 1133); *see also United States* v. *Willis*, 476 F.3d 1121, 1124-27 (10th Cir. 2007) (upholding a conviction for aiding and abetting access to a protected computer "without authorization" where an employee gave login credentials for a financial information website to an associate of his drug dealer who in turn used the accessed information for identity theft).

In the face of multiple circuits that agree with our plain meaning construction of the statute, the dissent would have us ignore common sense and turn the statute inside out. Indeed, the dissent frames the question upside down in assuming that permission from FH is at issue. Under this approach, ignoring reality and practice, an employee could undermine the company's ability to control access to its own computers by willy nilly giving out passwords to anyone outside the company—former employees whose access had been revoked, competitors, industrious hackers or bank robbers who find it less risky and more convenient to access accounts via the Internet rather than through armed robbery. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1179-80 (2016).

Our conclusion does nothing to expand the scope of violations under the CFAA beyond *Brekka*; nor does it rest on the grace of prosecutorial discretion. We are mindful of the examples noted in *Nosal I*—and reiterated by Nosal and various amici—that ill-defined terms may capture arguably innocuous conduct, such as password sharing among friends and family, inadvertently "mak[ing] criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Nosal I*, 676 F.3d at 859. But these concerns are ill-founded because § 1030(a)(4) requires access be "knowingly and with intent to defraud" and further, we have held that violating use restrictions, like a website's terms of use, is insufficient without more to form the basis for liability under the CFAA. *See Nosal I*, 676 F.3d at 862-63. The circumstance here—former employees whose computer access was categorically revoked and who surreptitiously

accessed data owned by their former employer—bears little resemblance to asking a spouse to log in to an email account to print a boarding pass. The charges at issue in this appeal do not stem from the ambiguous language of *Nosal I*—"exceeds authorized access"—or even an ambiguous application of the phrase "without authorization," but instead relate to the straightforward application of a common, unambiguous term to the facts and context at issue.

The *Brekka* analysis of the specific phrase "without authorization"—which is consistent with our sister circuits—remains controlling and persuasive. We therefore hold that Nosal, a former employee whose computer access credentials were affirmatively revoked by Korn/Ferry acted "without authorization" in violation of the CFAA when he or his former employee co-conspirators used the login credentials of a current employee to gain access to confidential computer data owned by the former employer and to circumvent Korn/Ferry's revocation of access.

C. Jury Instruction on "Without Authorization"

With respect to the meaning of "without authorization," the district court instructed the jury as follows:

> Whether a person is authorized to access the computers in this case depends on the actions taken by Korn/Ferry to grant or deny permission to that person to use the computer. A person uses a computer "without authorization" when the person has not received permission from Korn/Ferry to use the computer for any purpose (such as when a

> hacker accesses the computer without any permission), or when Korn/Ferry has rescinded permission to use the computer and the person uses the computer anyway.

The instruction is derived directly from our decision in *Brekka* and is a fair and accurate characterization of the plain meaning of "without authorization." Although the term "without authorization" is unambiguous, it does not mean that the facts don't matter; the source and scope of authorization may well be at issue. Here, it was not disputed that Korn/Ferry was the source of permission to grant authorization. The jury instruction left to the jury to determine whether such permission was given.

Nosal challenges the instruction on the basis that the CFAA only criminalizes access where the party circumvents a technological access barrier.[13] Not only is such a requirement missing from the statutory language, but it would make little sense because some § 1030 offenses do not require access to a computer at all. For example, § (a)(6) imposes penalties for trafficking in passwords "through which a computer can be accessed without authorization * * * ." 18 U.S.C. § 1030(a).

In any event, Nosal's argument misses the mark on the technological access point. Even if he were

---

[13] Nosal did not object to this instruction at the jury instruction conference. He did, however, raise the issue and offer a circumvention instruction earlier in the proceedings and objected to an earlier version of this instruction. Whether we review the instruction de novo or for plain error, the result is the same because the instruction was correct.

correct, any instructional error was without consequence in light of the evidence. The password system adopted by Korn/Ferry is unquestionably a technological barrier designed to keep out those "without authorization." Had a thief stolen an employee's password and then used it to rifle through Searcher, without doubt, access would have been without authorization.

The same principle holds true here. A password requirement is designed to be a technological access barrier.

D. Accomplice Liability Under the CFAA

Nosal's convictions under the CFAA rest on accomplice liability. Nosal claims the government failed to prove the requisite mens rea. Two instructions bear on this issue: aiding and abetting and deliberate ignorance. As to the former, which is not challenged on appeal, the court instructed that the government must prove Nosal "knowingly and intentionally aided, counseled, commanded, induced or procured [a] person to commit each element of the crime" and did so "before the crime was completed * * * with the knowledge and intention of helping that person commit the crime." The court also instructed that the defendant acted "knowingly" if he was "aware of the act and [did] not act or fail to act through ignorance, mistake, or accident." The adjunct deliberate ignorance instruction read: the defendant acted "knowingly" if he "was aware of a high probability that [Christian, Jacobson, or FH] had gained unauthorized access to a computer * * * or misappropriated trade secrets * * * without

authorization * * * and deliberately avoided learning the truth."

At trial, Nosal objected to the deliberate ignorance instruction on the ground that the facts alleged did not permit a deliberate ignorance theory. On appeal, for the first time, he argues that the instruction is erroneous because it undermines the requirement that Nosal had advance knowledge of the crime.[14] We review this challenge for plain error. *See Jones* v. *United States*, 527 U.S. 373, 388 (1999).

We have repeatedly held that a statutory requirement that a criminal defendant acted "knowingly" is "not limited to positive knowledge, but includes the state of mind of one who does not possess positive knowledge only because he consciously avoided it." *United States* v. *Heredia*, 483 F.3d 913, 918 (9th Cir. 2007) (internal citation and alterations omitted); *see also United States* v. *Jewell*, 532 F.2d 697, 700 (9th Cir. 1976) ("To act 'knowingly,' therefore, is not necessarily to act only with positive knowledge, but also to act with an awareness of the high probability of the existence of the fact in question. When such awareness is present, 'positive' knowledge is not required."). We have equated positive knowledge and deliberate ignorance in upholding conspiracy convictions and

[14] The district court accommodated Nosal's many objections to this instruction. In particular, at his request, the instruction included the names of the co-conspirators. When the court asked if this included "the three people," Nosal's counsel said, "Right." The instruction thus incorporated, with no further objection or comment, FH's name. Nosal thus waived any challenge to inclusion of her name, which was not plain error in any event.

see no reason to distinguish aiding and abetting liability. *See, e.g.*, *United States* v. *Ramos-Atondo*, 732 F.3d 1113, 1120 (9th Cir. 2013) (holding the district court did not abuse its discretion by instructing the jury on a theory of deliberate ignorance in the context of a conspiracy to import marijuana as "'[t]he *Jewell* standard eliminates the need to establish such positive knowledge to obtain a conspiracy conviction'" (alterations in original) (quoting *United States* v. *Nicholson*, 677 F.2d 706, 711 (9th Cir. 1982))).

Nor does the recent case *Rosemond* v. *United States* counsel a different result. 134 S. Ct. 1240 (2014). In *Rosemond*, the Supreme Court held that an accomplice must have "advance knowledge" of the crime the principal is planning to commit, "knowledge that enables him to make the relevant legal (and indeed, moral) choice." *Id.* at 1249. Nosal argues that the district court erred in not including *Rosemond*'s advance knowledge requirement. But as the Supreme Court notes, an advance knowledge requirement for accomplice liability is not new. *Id.* at 1248-49. Nothing in *Rosemond* suggests that the Court foreclosed a deliberate ignorance instruction, which was not an issue in the case. Instead, *Rosemond* focuses on when a defendant must have advance knowledge, meaning "knowledge at a time the accomplice can do something with it—most notably, opt to walk away." *Id*. at 1249-50. The instructions here are perfectly consonant with our line of cases extending back to *Jewell*. If the Supreme Court had chosen to overturn decades of jurisprudence, we would expect clearer direction. *See United States* v. *Ford*, 821 F.3d 63, 74 (1st Cir. 2016) (holding that "willful blindness," including

ignoring "red flags," meets the mens rea element of aiding and abetting liability, and discussing the impact of *Rosemond* elsewhere in the opinion).

Apart from the instruction, Nosal challenges the sufficiency of the evidence, claiming evidence of intent was insufficient because he didn't have advance knowledge that Christian and Jacobson would use FH's password. This attack fails because, "after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson* v. *Virginia*, 443 U.S. 307, 319 (1979) (emphasis in original). Extensive testimony revealed that Nosal wanted his team to obtain information from Searcher all while maintaining his distance from their activities.

Although the conviction may be upheld solely under *Pinkerton*, which "'renders all co-conspirators criminally liable for reasonably foreseeable overt acts committed by others in furtherance of the conspiracy,'" *United States* v. *Bingham*, 653 F.3d 983, 997 (9th Cir. 2011) (quoting *United States* v. *Hernandez-Orellana*, 539 F.3d 994, 1006-07 (9th Cir. 2008)), sufficient evidence independently supports the aiding and abetting counts.

Christian's testimony is illustrative:

> Q. Did the defendant know you were using [FH's] password, after you left Korn/Ferry, to get source lists and other documents from Korn/Ferry?
>
> A. Yes.
>
> Q. Any doubt in your mind that he knew that?

A. No.

This unequivocal statement, which more than satisfies the *Jackson* v. *Virginia* standard, is bolstered by other evidence, including extensive testimony that Nosal wanted his team to obtain information from Searcher while maintaining his distance from their activities but knew and understood that none of them had access credentials. A juror also could have easily surmised that Nosal, having worked with FH for years on a daily basis, would have known that she had herself never run custom reports, developed source lists or pulled old source lists. When Nosal specifically directed Christian to access Korn/Ferry's computer system to "[g]et what I need," Nosal knew that the only way Christian and Jacobson could access the source lists was "without authorization" because Korn-Ferry had revoked their access credentials.

We affirm Nosal's conviction on the CFAA counts.

II. CONVICTIONS UNDER THE ECONOMIC ESPIONAGE ACT (EEA)

The jury convicted Nosal of two counts of trade secret theft under the EEA: Count 5 charged "unauthorized downloading, copying and duplicating of trade secrets" in violation of 18 U.S.C. §§ 1832(a)(2) & (a)(4); and Count 6 charged unauthorized receipt and possession of stolen trade secrets in violation of 18 U.S.C. § 1832(a)(3) & (a)(4). Both counts relate to Christian's use of FH's login credentials to obtain three source lists of CFOs from Searcher. Count 6 also included a "cut and paste" of a list of executives derived from Searcher. Christian emailed Nosal the resulting lists, which contained

candidate names, company positions and phone numbers. Nosal primarily challenges the sufficiency of the evidence on the trade secret counts.

A. Sufficiency of the Evidence—Counts 5 and 6

Violation of the EEA requires, among other things, "intent to convert a trade secret" and "intending or knowing that the offense will[] injure [an] owner of that trade secret * * * ." 18 U.S.C. § 1832(a). The jury instruction for Count 5—downloading, copying and duplicating trade secrets—set out the following elements:

1. At least one of the three source lists is a trade secret (requiring agreement on which one);

2. Nosal knew that the source list was a trade secret;

3. Nosal knowingly, and without authorization, downloaded, copied or duplicated the trade secret;

4. Nosal intended to convert the trade secret to the economic benefit of someone other than the owner;

5. Nosal knew or intended that the offense would injure the trade secret owner; and

6. The trade secret was related to or included in a product in interstate commerce.

The instruction for Count 6—receiving and possessing trade secrets—replaced the third element with a requirement of knowing receipt or possession

of a trade secret with the knowledge that it was "stolen or appropriated, obtained, or converted without authorization" and added the "cut and paste" list as one of the possible trade secrets.

Nosal argues that the government failed to prove: 1) secrecy and difficulty of development, because the search information was derived from public sources and because there was no evidence the source lists had not been circulated outside Korn/Ferry; 2) knowledge of trade secret status; and 3) knowledge of injury to, or an intent to injure, Korn/Ferry.

The notion of a trade secret often conjures up magic formulas, like Coca Cola's proprietary formula, technical drawings or scientific data. So it is no surprise that such technically complex cases have been brought under the EEA. *See, e.g.*, *United States* v. *Chung*, 659 F.3d 815, 819 (9th Cir. 2011) (documents related to space shuttles and rockets); *United States* v. *Yang*, 281 F.3d 534, 540 (6th Cir. 2002) (scientific research in adhesives); *United States* v. *Hsu*, 155 F.3d 189, 191-92 (3d Cir. 1998) (processes, methods and formulas for manufacturing an anti-cancer drug).

But the scope of the EEA is not limited to these categories and the EEA, by its terms, includes financial and business information. The EEA defines a trade secret as

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including * * * compilations * * * if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent

> economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public * * * .

18 U.S.C. § 1839(3).[15]

The thrust of Nosal's argument is that the source lists are composed largely, if not entirely, of public information and therefore couldn't possibly be trade secrets. But he overlooks the principle that a trade secret may consist of a compilation of data, public sources or a combination of proprietary and public sources. It is well recognized that

> it is the secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation, or integration of the individual elements. * * * [T]he theoretical possibility of reconstructing the secret from published materials containing scattered references to portions of the information or of extracting it from public materials unlikely to come to the attention of the appropriator will not preclude relief against the wrongful conduct * * * .

Restatement (Third) of Unfair Competition § 39 cmt. f (1995); *see also Computer Care* v. *Serv.*

---

[15] This was the text of § 1839 at the time the offenses were committed. Congress recently amended § 1839, replacing "the public" with "another person who can obtain economic value from the disclosure or use of the information." Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2(b)(1)(A), 130 Stat. 376, 380.

Sys. Enters., Inc., 982 F.2d 1063, 1074 (7th Cir. 1992) ("A trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process design and operation of which in unique combination affords a competitive advantage and is a protectable trade secret" (internal citation omitted)); *Boeing Co.* v. *Sierracin Corp.*, 738 P.2d 665, 675 (Wash. 1987) (holding that "trade secrets frequently contain elements that by themselves may be in the public domain but together qualify as trade secrets"). Expressed differently, a compilation that affords a competitive advantage and is not readily ascertainable falls within the definition of a trade secret.

The source lists in question are classic examples of a trade secret that derives from an amalgam of public and proprietary source data. To be sure, some of the data came from public sources and other data came from internal, confidential sources. But cumulatively, the Searcher database contained a massive confidential compilation of data, the product of years of effort and expense. Each source list was the result of a query run through a propriety algorithm that generates a custom subset of possible candidates, culled from a database of over one million executives. The source lists were not unwashed, public-domain lists of all financial executives in the United States, nor otherwise related to a search that could be readily completed using public sources. Had the query been "who is the CFO of General Motors" or "who are all of the CFOs in a particular industry," our analysis might be different. Instead, the nature of the trade secret and its value stemmed from the unique integration,

compilation, cultivation, and sorting of, and the aggressive protections applied to, the Searcher database.

Nosal takes the view that the source lists are merely customer lists that cannot be protected as trade secrets. This characterization attempts to sidestep the unique nature of the source lists, which are the customized product of a massive database, not a list of well-known customers. Regardless, courts have deemed customer lists protectable trade secrets. *See, e.g.*, *Hollingsworth Solderless Terminal Co.* v. *Turley*, 622 F.2d 1324, 1332-33 (9th Cir. 1980) (setting out in detail how to analyze whether a customer list is a trade secret); *Hertz* v. *Luzenac Grp.*, 576 F.3d 1103, 1114 (10th Cir. 2009) (holding that a customer list may be a trade secret where "it is the end result of a long process of culling the relevant information from lengthy and diverse sources, even if the original sources are publicly available").

Our approach is not novel. This case is remarkably similar to *Conseco Finance Servicing Corp.* v. *North American Mortgage Co.*, 381 F.3d 811 (8th Cir. 2004). Conseco was a financial services company that issued subprime mortgages. *Id.* at 814. It generated potential customer leads through a database of information on over 40 million individuals. *Id.* at 815. A computer program compiled lists of potential customers, which were sent to branch offices as "customer lead sheets," coded from most promising (red) to decent (blue). *Id.* Several departing staff took copies of the lead sheets and went to work for a competitor. *Id.* at 816. Even though all the information in the lead sheets was public, the Eighth

Circuit held that they were trade secrets: they "are a product of a specialized—and apparently quite effective—computer program that was uniquely Conseco's." *Id.* at 819.[16]

Nosal also takes aim at the secrecy of the three source lists in question, an argument that is intertwined with his public domain/compilation claim. The jury heard more than enough evidence to support the verdict. Christian acknowledged that the only place she could obtain the source lists she needed was on Korn/Ferry's computer system. Notably, some of the downloaded information came from a source list for an engagement that was opened only twelve days prior to the April 12 downloads underlying the trade secret counts.

Although Nosal claims that Korn/Ferry's sharing of lists with clients and others undermined this claim of secrecy, witnesses who worked at Korn/Ferry did not budge in terms of procedures undertaken to keep the data secret, both in terms of technology protections built into the computer system and the limitations on distribution of the search results. For example, the Vice-President of Information Services testified that, to her knowledge, the source lists had never been released by Korn/Ferry to any third parties. As a matter of practice, Korn/Ferry did not show source lists to clients. In the occasional instance when a

---

[16] *See also Rivendell Forest Prods., Ltd.* v. *Ga.-Pac. Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994) (defining a trade secret as including "a system where the elements are in the public domain, but there has been accomplished an effective, successful and valuable integration of the public domain elements and the trade secret gave the claimant a competitive advantage which is protected from misappropriation").

client was given a source list or shown one at a pitch, it was provided on an understanding of confidentiality, and disclosing the lists was contrary to company policy. It is also well established that "confidential disclosures to employees, licensees, or others will not destroy the information's status as a trade secret." Restatement (Third) of Unfair Competition § 39 cmt. f (1995).

In light of the above, it would be naive to conclude that Nosal was unaware that the information pirated by Christian included trade secrets or that the piracy would harm Korn/Ferry. As a former senior executive at Korn/Ferry, Nosal was deeply familiar with the competitive advantage Searcher provided, and was cognizant of the measures the company took to protect the source lists generated. He signed a confidentiality agreement stating that "information databases and company records are extremely valuable assets of [Korn/Ferry's] business and are accorded the legal protection applicable to a company's trade secrets." The source lists were also marked "Korn/Ferry Proprietary & Confidential." While a label or proprietary marking alone does not confer trade secret status, the notice and protective measures taken by Korn/Ferry significantly undermine Nosal's claim he was unaware the source lists were trade secret information.

Nosal's argument that he and his colleagues were unaware their actions would harm Korn/Ferry also holds no water. They launched a direct competitor to Korn/Ferry and went to great lengths to access the source lists, fully aware of the competitive advantage Searcher gave Korn/Ferry as they attempted to populate their own database. Christian underscored

the value of the lists through her testimony that she and Nosal used the source lists to complete searches faster and gain credibility with clients. They recognized that the required substantial investment of time, money and elbow grease to even try to replicate the source lists would have destroyed their prime value—immediacy.

At trial, Nosal's counsel endeavored to attack the secrecy, knowledge and other elements of the trade secret counts. The jury heard extensive testimony and argument. Construing the evidence in the light most favorable to the government, a rational juror could have concluded that the evidence supported convictions under §§ 1832(a)(2), (3) and (4) of the EEA. As the Supreme Court explained just this year, our "limited review does not intrude on the jury's role 'to resolve conflicts in the testimony, to weigh the evidence, and to draw reasonable inferences from basic facts to ultimate facts.'" *Musacchio*, 136 S. Ct. at 715 (quoting *Jackson*, 443 U.S. at 319). It was no stretch for the jury to conclude that the source lists were trade secrets, that Nosal knew they were trade secrets and that Nosal knew stealing the source lists would harm Korn/Ferry by helping a competitor—Nosal's own company.

B. Conspiracy Jury Instruction

With respect to trade secrets, the conspiracy jury instruction stated that "the government need not prove the existence of actual trade secrets and that Defendant knew that the information in question was a trade secret. However, the government must prove that Defendant firmly believed that certain

information constituted trade secrets." Nosal argues that the court constructively amended the indictment because the indictment alleges theft of actual trade secrets while the jury instruction did not require proof of actual trade secrets. Constructive amendment occurs where "the crime charged is substantially changed at trial, so that it is impossible to know whether the grand jury would have indicted for the crime actually proved." *United States* v. *Howick*, 263 F.3d 1056, 1063 (9th Cir. 2001) (citations and alterations omitted). Here, there was no constructive amendment. In indicting Nosal for theft of trade secrets under 18 U.S.C. § 1832(a), the grand jury necessarily considered whether Nosal "knowingly" stole the source lists; "firmly believed" is a lesser standard. A grand jury that indicted on this more inclusive "knowing" standard would necessarily have indicted on this lesser standard.

In a related vein, Nosal claims that the instruction unfairly removes the requirement to prove an actual trade secret. The instruction reflects our circuit's precedent on conspiracy charges—a conviction may be upheld even where the object of the crime was not a legal possibility. *See United States* v. *Rodriguez*, 360 F.3d 949, 957 (9th Cir. 2004) (upholding convictions for conspiracy to rob cocaine traffickers where "neither the narcotics nor the narcotics traffickers actually existed" since "[i]mpossibility is not a defense to [a] conspiracy charge"). We agree with the other circuits that have applied this same principle to trade secrets. *See Yang*, 281 F.3d at 544 (holding that the government did not need to prove theft of actual trade secrets because the defendants "intended to commit the crime and took a substantial step towards commission of the crime"); *United*

States v. *Martin*, 228 F.3d 1, 13 (1st Cir. 2000) (holding the "key question is whether [the defendant] intended to steal secrets," not whether he actually did); *Hsu*, 155 F.3d at 204 ("A defendant can be convicted of attempt or conspiracy pursuant to 18 U.S.C. §§ 1832(a)(4) or (a)(5) even if his intended acts were legally impossible."). In any event, the jury found theft of actual trade secrets, and therefore any error was harmless. *See Neder* v. *United States*, 527 U.S. 1, 19 (1999).

C. Evidentiary Challenges

Nosal disputes evidentiary rulings made regarding his non-competition agreement. Although Nosal was permitted to testify that he believed the agreement was illegal, the court struck certain testimony by government witnesses about the agreement and also precluded evidence about the enforceability of the agreement under California law. The jury was instructed that whether "Mr. Nosal breached or did not breach this covenant is not relevant to the question of whether he is guilty of the crimes charged in this case." The district court did not abuse its discretion.

In closing rebuttal, the government argued that Nosal's use of the name "David Nelson" showed his intent to conspire to steal information from Korn/Ferry. Importantly, the government did not link Nosal's charade to the legality of the non-competition agreement. This passing reference, which was not objected to at trial, was harmless and certainly does not rise to the level of plain error.

III. RESTITUTION ORDER

The district court awarded Korn/Ferry $827,983.25 in restitution. We review de novo the legality of the restitution order and review for clear error the factual findings that support the order. *United States* v. *Luis*, 765 F.3d 1061, 1065 (9th Cir. 2014), *cert. denied*, 135 S. Ct. 1572 (2015) (citations omitted). If the order is "'within the bounds of the statutory framework, a restitution order is reviewed for abuse of discretion.'" *Id.* (citation omitted).

The restitution order identified three categories of recoverable losses: 1) Korn/Ferry's internal investigation costs incurred in attempting to ascertain the nature and scope of Nosal's breach, in the amount of $27,400; 2) the value of Korn/Ferry's employee time spent participating in and assisting the government's investigation and prosecution, in the amount of $247,695; and 3) the attorneys' fees incurred by Korn/Ferry in aid of the investigation or prosecution of the offense, in the amount of $595,758.25. While the government asked for a higher amount, the district court reduced the award, primarily by cutting the request for attorneys' fees from $964,929.65 to $595,758.25 for invoices "not demonstrably reasonably necessary to the government's investigation and prosecution," for "staffing inefficiencies," and for "time spent on 'press' and file/order reviewing charges."

The district court relied on the Mandatory Victim Restitution Act (MVRA), which "makes restitution mandatory for particular crimes, including those offenses which involve fraud or deceit." *United States* v. *Gordon*, 393 F.3d 1044, 1048 (9th Cir. 2004)

(citing 18 U.S.C. § 3663A(c)(1)(A)(ii)). The MVRA requires that restitution awards "reimburse the victim for lost income and necessary child care, transportation, and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense." 18 U.S.C. § 3663A(b)(4). Although the MVRA was passed as part of the Violence Against Women Act and directed in part to concerns related to women victims of crime, such as child care costs, *see* Pub. L. 103-322, § 40504, 108 Stat. 1796, 1947 (1994), we have joined other circuits in holding that the language "other expenses incurred during the participation in the investigation or prosecution" also authorizes the award of investigation costs and attorneys' fees in some circumstances. *See, e.g.*, *United States* v. *Abdelbary*, 746 F.3d 570, 574-79 (4th Cir. 2014); *United States* v. *Elson*, 577 F.3d 713, 728 (6th Cir. 2009); *United States* v. *Waknine*, 543 F.3d 546, 558-59 (9th Cir. 2008); *United States* v. *Amato*, 540 F.3d 153, 159-62 (2d Cir. 2008); *Gordon*, 393 F.3d at 1056-57.

We must initially decide whether, as Nosal urges, the restitution award is invalid because it exceeds the actual loss that the district court determined for the purposes of the Sentencing Guidelines U.S.S.G. § 2B1.1(b)—calculated at $46,907.88. The answer to that question is found in our observation that "calculating loss under the guidelines is not necessarily identical to loss calculation for purposes of restitution." *United States* v. *Hunter*, 618 F.3d 1062, 1065 (9th Cir. 2010). Rather, restitution loss is governed not by the criteria of the Sentencing Guidelines, but by the MVRA's purpose of "mak[ing] the victim[] whole." *Gordon*, 393 F.3d at 1052 n.6.

To this end, the plain language of 18 U.S.C. § 3663A(a)(1) makes restitution mandatory "[n]otwithstanding any other provision of law" and "in addition to * * * any other penalty authorized by law," including the Sentencing Guidelines. *See also Amato*, 540 F.3d at 160-62.

In contrast with the MVRA, which includes expenses related to investigation and prosecution, such costs are categorically excluded under the Sentencing Guidelines applicable here. The guidelines provision for actual loss for crimes of fraud explicitly excludes "costs incurred by victims primarily to aid the government in[] the prosecution and criminal investigation of an offense." U.S.S.G. § 2.B.1.1 cmt. 3(D)(ii). From that, Nosal appears to assume, without any support, that "actual loss" is a term-of-art, such that in this category of offenses a restitution order could never include investigation costs or attorneys' fees in aid of the government. That assumption is not warranted under the plain language of the MVRA, which notably never uses the terminology of actual loss.

In an effort to overcome the differences between the MVRA and the guidelines, Nosal points to our decision in *United States* v. *Stoddard*, 150 F.3d 1140, 1147 (9th Cir. 1998), which states that "[r]estitution can only be based on actual loss." We acknowledge that *Stoddard*'s use of the phrase "actual loss" in discussion of restitution generates some confusion, but *Stoddard* does not answer the question at hand. In *Stoddard*, the difference between the loss under the Sentencing Guidelines and the restitution award ($30,000 versus $116,223) related to profits that the defendant received from a business opportunity

linked to the fraud, not for anything remotely resembling the investigation costs at issue here. *See id.* at 1147-48 (Ferguson, J., dissenting).

Nosal is also mistaken that this reading of the statute creates a circuit split with the Seventh Circuit. *See United States* v. *Dokich*, 614 F.3d 314, 318-20 (7th Cir. 2010). *Dokich* addressed whether a $55.9 million restitution award was calculated using intended loss or actual loss. Based on an unclear record, the court was forced to conclude that the restitution award (which was higher than the $20-$50 million loss used for sentencing under the guidelines) was based on intended loss, not actual loss, and therefore barred. *Id.* As in *Stoddard*, the case had nothing to do with inclusion of investigation costs as part of the restitution loss calculation.

Having determined that the restitution award was "within the bounds of the statutory framework," we turn to whether the district court nevertheless abused its discretion in awarding nearly $1 million in restitution. *See Waknine*, 543 F.3d at 555 (quoting *Gordon*, 393 F.3d at 1051). With respect to investigation costs and attorneys' fees, our rule is clear: restitution for such losses "'may be recoverable'" where the harm was the "'direct and foreseeable result' of the defendant's wrongful conduct * * *." *Gordon*, 393 F.3d at 1057 (quoting *United States* v. *Phillips*, 367 F.3d 846, 863 (9th Cir. 2004)). *But see Amato*, 540 F.3d at 162 (disagreeing with *Gordon*'s approach of basing restitution on the foreseeable results of the criminal conduct). We require the government to present evidence "demonstrat[ing] that it was reasonably necessary for [the victim] to incur attorneys' and investigator's

fees to participate in the investigation or prosecution of the offense." *Waknine*, 543 F.3d at 559. Unlike some other circuits, *see, e.g.*, *United States* v. *Papagno*, 639 F.3d 1093, 1099-1100 (D.C. Cir. 2011), we have "'adopted a *broad* view of the restitution authorization [for investigation costs].'" *Gordon*, 393 F.3d at 1056-57 (alteration in original) (quoting *Phillips*, 367 F.3d at 863).

We applaud the district court's thorough review of the voluminous time and fee records submitted by the government and Korn/Ferry. We agree with the award for internal investigation costs to uncover the extent of the breach and for the value of employee time spent participating in the government's investigation and prosecution. *See, e.g.*, *United States* v. *De La Fuente*, 353 F.3d 766, 773 (9th Cir. 2003) (upholding an award for a "cleanup and decontamination" costs in response to an anthrax scare); *United States* v. *Hosking*, 567 F.3d 329, 332 (7th Cir. 2009) (holding that restitution included the value of "[t]he time and effort spent by the bank's employees and outside professionals in unraveling the twelve-year embezzlement scheme"). However, we part ways with the district court and the government with respect to Korn/Ferry's attorneys' fees.

While the district court's reduction of the fee award was a step in the right direction, our review of the record convinces us that the court should have gone further. Several principles guide this conclusion. To begin, the fees must be the direct and foreseeable result of the defendant's conduct. *Gordon*, 393 F.3d at 1057 (quoting *Phillips*, 367 F.3d at 863). Next, as in other attorneys' fee awards, reasonableness is the

touchstone. Reasonableness is benchmarked against the necessity of the fees under the terms of the statute, thus excluding duplicate effort, time that is disproportionate to the task and time that does not fall within the MVRA's mandate.[17] Finally, fees are only recoverable if incurred during "*participation in* the investigation or prosecution of the offense." 18 U.S.C. § 3663A(b)(4) (emphasis added). The company's attorneys are not a substitute for the work of the prosecutor, nor do they serve the role of a shadow prosecutor. To be sure, nothing is wrong with proactive participation. But participation does not mean substitution or duplication.

Even after reduction, the total amount of fees awarded is striking, particularly given that the trial ultimately involved only three discrete incidents of criminal behavior. Although resulting in multiple counts, at bottom the events were temporally circumscribed and limited in scope. We note that a highly disproportionate percentage of the fees arose from responding to requests and inquiries related to sentencing, damages, and restitution. The reasonableness of the fees needs to be reexamined to consider (i) whether the sizeable fee related to restitution matters was reasonable; (ii) whether there was unnecessary duplication of tasks between Korn/Ferry staff and its attorneys since the court awarded a substantial sum for the time of Korn/Ferry employees; and (iii) whether the outside attorneys were substituting for or duplicating the

[17] We agree with the district court's decision to accept the hourly rate of Korn/Ferry's attorneys. Recognizing the importance and impact of the breach, Korn/Ferry cannot be faulted for selecting an "excellent," or "premium," law firm.

work of the prosecutors, rather than serving in a participatory capacity.

We vacate the restitution award with respect to the attorneys' fees and remand for reconsideration in light of the principles and observations set out above.

AFFIRMED, EXCEPT VACATED IN PART AND REMANDED WITH RESPECT TO THE RESTITUTION AWARD.

REINHARDT, Circuit Judge, dissenting:

This case is about password sharing. People frequently share their passwords, notwithstanding the fact that websites and employers have policies prohibiting it. In my view, the Computer Fraud and Abuse Act ("CFAA") does not make the millions of people who engage in this ubiquitous, useful, and generally harmless conduct into unwitting federal criminals. Whatever other liability, criminal or civil, Nosal may have incurred in his improper attempt to compete with his former employer, he has not violated the CFAA.

The first time this case came before us we examined whether Nosal's former colleagues acted "without authorization, or exceed[ed] authorized access" when they downloaded information from Searcher while still employed at Korn/Ferry and shared it with Nosal in violation of the firm's policies. *United States* v. *Nosal (Nosal I)*, 676 F.3d 854, 864 (9th Cir. 2012) (en banc). We said "no," rejecting the approach of a few other circuits which had interpreted the CFAA looking "only at the culpable behavior of the defendants before them, and fail[ing] to consider the effect on millions of ordinary citizens." *Id.* at 862. In doing so, we stated that they turned the CFAA into a "sweeping Internet-policing mandate," instead of maintaining its "focus on hacking." *Id.* at 858. We emphatically refused to turn violations of use restrictions imposed by employers or websites into crimes under the CFAA, declining to put so many citizens "at the mercy of [their] local prosecutor." *Id.* at 862. Since then, both circuits to rule on the point have agreed with our interpretation. *See United States* v. *Valle*, 807 F.3d

508, 526-28 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC* v. *Miller*, 687 F.3d 199, 204 (4th Cir. 2012).

Today, addressing only slightly different conduct, the majority repudiates important parts of *Nosal I*, jeopardizing most password sharing. It loses sight of the anti-hacking purpose of the CFAA, and despite our warning, threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens.

At issue are three incidents of password sharing. On these occasions while FH was still employed at Korn/Ferry, she gave her password to Jacobson or Christian, who had left the company. Her former colleagues then used her password to download information from Searcher. FH was authorized to access Searcher, but she did not download the information herself because it was easier to let Jacobson or Christian do it than to have them explain to her how to find it. It would not have been a violation of the CFAA if they had simply given FH step-by-step directions, which she then followed. Thus the question is whether because Jacobson and Christian instead used FH's password with her permission, they are criminally liable for access "without authorization" under the Act.[1]

The majority finds the answer is "yes," but in doing so commits the same error as the circuits whose views we rejected in *Nosal I*. My colleagues claim that they do not have to address the effect of their

[1] Nosal was charged as criminally culpable for Jacobson's and Christian's alleged violations under a theory of either aiding and abetting or conspiracy.

decision on the wider population because Nosal's infelicitous conduct "bears little resemblance" to everyday password sharing. Notably this is the exact argument the *dissent* made in *Nosal I*: "This case has nothing to do with playing sudoku, checking email, [or] fibbing on dating sites * * * . The role of the courts is neither to issue advisory opinions nor to declare rights in hypothetical cases." 676 F.3d at 864, 866 (Silverman, J., dissenting) (internal quotation and citation omitted).

We, of course, rejected the dissent's argument in *Nosal I*. We did so because we recognized that the government's theory made all violations of use restrictions criminal under the CFAA, whether the violation was innocuous, like checking your personal email at work, or more objectionable like that at issue here. Because the statute was susceptible to a narrower interpretation, we rejected the government's broader reading under which "millions of unsuspecting individuals would find that they are engaging in criminal conduct." *Id.* at 859. The same is true here. The majority does not provide, nor do I see, a workable line which separates the consensual password sharing in this case from the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners. There simply is no limiting principle in the majority's world of lawful and unlawful password sharing.

Therefore, despite the majority's attempt to construe *Nosal I* as only applicable to "exceeds authorized access," the case's central lesson that the CFAA should not be interpreted to criminalize the ordinary conduct of millions of citizens applies

equally strongly here. Accordingly, I would hold that consensual password sharing is not the kind of "hacking" covered by the CFAA. That is the case whether or not the voluntary password sharing is with a former employee and whether or not the former employee's own password had expired or been terminated.

I.

"Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking," *Nosal I*, 676 F.3d at 858. *United States* v. *Morris*, the first appellate case under the CFAA, illustrates the core type of conduct criminalized by the Act. 928 F.2d 504 (2d Cir. 1991). There a student created a worm which guessed passwords and exploited bugs in computer programs to access military and university computers, eventually causing them to crash. The Second Circuit found that the student had accessed those computers "without authorization" in violation of the Act. *Id*. at 506, 509-511.

"Without authorization" is used in a number of places throughout the CFAA, but is not defined in the Act. The phrase appears in two subsections relevant to this case: § 1030(a)(2)(C) and (a)(4). Subsection (a)(2)(C) criminalizes "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] * * * information from any protected computer." This is the "broadest provision" of the CFAA. *Nosal I*, 676 F.3d at 859. Subsection (a)(4) in essence increases the penalty for violating (a)(2)(C) if the perpetrator also acts "with intent to defraud,"

and "obtains anything of value."[2] Nosal was charged and convicted under (a)(4).

Our definition of "without authorization" in this case will apply not only to (a)(4), but also to (a)(2)(C) and the rest of the Act. In *Nosal I*, the government contended that "exceeds authorization" could be interpreted more narrowly in (a)(2)(C) than in (a)(4), but we concluded: "This is just not so: Once we define the phrase for the purpose of subsection 1030(a)(4), 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.'" 676 F.3d at 859 (quoting *Powerex Corp.* v. *Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)). That holds here. Indeed, the government so concedes.

It is thus necessary to consider the potential breadth of subsection (a)(2)(C) if we construe "without authorization" with less than the utmost care. Subsection (a)(2)(C) criminalizes nearly all intentional access of a "protected computer" without authorization.[3] A "'protected computer' is defined as

---

[2] The penalty for violating § 1030(a)(2)(C) may also be increased if the government proves an additional element under (c)(2)(B).

[3] Computer is defined under the Act as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1). *See also United States* v. *Mitra*, 405 F.3d 492 (7th Cir. 2005) (finding a radio system is a computer); *United States* v. *Kramer*, 631 F.3d 900, 902 (8th Cir. 2011) (noting the Act's definition of a

a computer affected by or involved in interstate commerce—effectively all computers with Internet access." *See Nosal I*, 676 F.3d at 859. This means that nearly all desktops, laptops, servers, smartphones, as well as any "iPad, Kindle, Nook, X-box, Blu-Ray player or any other Internet-enabled device," including even some thermostats qualify as "protected." *Id.* at 861. Thus § 1030(a)(2)(C) covers untold millions of Americans' interactions with these objects every day. Crucially, violating (a)(2)(C) does not require "any culpable intent." *Id*. Therefore if we interpret "without authorization" in a way that includes common practices like password sharing, millions of our citizens would become potential federal criminals overnight.

II.

The majority is wrong to conclude that a person necessarily accesses a computer account "without authorization" if he does so without the permission of the system owner.[4] Take the case of an office worker asking a friend to log onto his email in order to print

---

computer "is exceedingly broad," and concluding an ordinary cell phone is a computer).

To violate § 1030(a)(2)(C) a person must also "obtain information," but it is nearly impossible to access a computer without also obtaining information. As we noted in *Nosal I*, obtaining information includes looking up a weather report, reading the sports section online, etc. *See also* Sen. Rep. No. 104-357, at 7 (1996) ("'[O]btaining information' includes merely reading it.").

[4] The term "system owner" refers to the central authority governing user accounts, whether the owner of a single computer with one or several user accounts, a workplace network with dozens, or a social networking site, bank website, or the like, with millions of user accounts.

a boarding pass, in violation of the system owner's access policy; or the case of one spouse asking the other to log into a bank website to pay a bill, in violation of the bank's password sharing prohibition. There are other examples that readily come to mind, such as logging onto a computer on behalf of a colleague who is out of the office, in violation of a corporate computer access policy, to send him a document he needs right away. "Facebook makes it a violation of the terms of service to let anyone log into your account," we noted in *Nosal I*, but "it's very common for people to let close friends and relatives check their email or access their online accounts." 676 F.3d at 861 (citing Facebook Statement of Rights and Responsibilities § 4.8).[5]

Was access in these examples authorized? Most people would say "yes." Although the system owners' policies prohibit password sharing, a legitimate account holder "authorized" the access. Thus, the best reading of "without authorization" in the CFAA is a narrow one: a person accesses an account "without authorization" if he does so without having the permission of *either* the system owner *or* a legitimate account holder.

This narrower reading is more consistent with the purpose of the CFAA. The CFAA is essentially an anti-hacking statute, and Congress intended it as

---

[5] For example, a recent survey showed that 46% of parents have the password to their children's social networking site, despite the fact that the largest site, Facebook, forbids password sharing. See USC Annenberg School Center for the Digital Future, *2013 Digital Future Report* 135 (2013), http://www.digitalcenter.org/wp-content/uploads/2013/06/20 13-Report.pdf.

such. *Nosal I*, 676 F.3d at 858. Under the preferable construction, the statute would cover only those whom we would colloquially think of as hackers: individuals who steal or guess passwords or otherwise force their way into computers without the consent of an authorized user, not persons who are given the right of access by those who themselves possess that right. There is no doubt that a typical hacker accesses an account "without authorization": the hacker gains access without permission – *either* from the system owner *or* a legitimate account holder. As the 1984 House Report on the CFAA explained, "it is noteworthy that Section 1030 deals with an unauthorized access concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering.'" H.R. Rep. 98-894, 20, 1984 U.S.C.C.A.N. 3689, 3706. We would not convict a man for breaking and entering if he had been invited in by a houseguest, even if the homeowner objected. Neither should we convict a man under the CFAA for accessing a computer account with a shared password with the consent of the password holder.

Nosal's conduct was, of course, unscrupulous. Nevertheless, as the Second Circuit found in interpreting the CFAA, "whatever the apparent merits of imposing criminal liability may seem to be *in this case*, we must construe the statute knowing that our interpretation of [authorization] will govern many other situations." *Valle*, 807 F.3d at 528. The construction that we adopt in Nosal's case will apply with equal force to all others, and the reading of "without authorization" we adopt for subsection (a)(4) will apply with equal force to subsection (a)(2)C). I would, therefore, hold that however

reprehensible Nosal's conduct may have been, he did not violate the CFAA.

III.

The majority insists that the text of the statute requires its broad construction, but that is simply not so. Citing our decision in *Brekka*, the majority defines "authorization" as "permission or power granted by an authority." After appealing to "ordinary meaning," "common sense meaning," and multiple dictionaries to corroborate this definition, the majority asserts that the term is "not ambiguous."

The majority is wrong. The majority's (somewhat circular) dictionary definition of "authorization" – "permission conferred by an authority" – hardly clarifies the meaning of the text. While the majority reads the statute to criminalize access by those without "permission conferred by" the system owner, it is also proper (and in fact preferable) to read the text to criminalize access only by those without "permission conferred by" either a legitimate account holder or the system owner. The question that matters is not what authorization *is* but who is entitled to give it. As one scholar noted, "there are two parties that have plausible claims to [give] authorization: the owner/operator of the computer, and the legitimate computer account holder." Orin S. Kerr, *Computer Crime Law* 48 (3d ed. 2013). Under a proper construction of the statute, either one can give authorization.

The cases the majority cites to support its contention that the statute's text requires a broad construction merely repeat dictionary definitions of

"without authorization." Those cases do nothing to support the majority's position that authorization can be given only by the system owner. The Fourth Circuit, quoting the *Oxford English Dictionary*, found that "based on the ordinary, contemporary, common meaning of 'authorization," an employee "accesses a computer 'without authorization' when he gains admission to a computer without approval." *WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F.3d 199, 204 (4th Cir. 2012). The Sixth Circuit, also quoting the *Oxford English Dictionary*, explained that "[t]he plain meaning of 'authorization' is '[t]he conferment of legality'" and concluded that "a defendant who accesses a computer 'without authorization' does so without sanction or permission." *Pulte Homes, Inc.* v. *Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 303-04 (6th Cir 2011). In both of these cases, the important question in Nosal's case – authorization from whom – went unanswered. The Second Circuit consulted the *Random House Dictionary* instead and concluded that the "common usage of 'authorization' suggests that one 'accesses a computer without authorization' if he accesses a computer without permission to do so *at all*." *Valle*, 807 F.3d 508, 524 (2nd Cir. 2015) (emphasis added). With that, I agree. Contrary to the majority's suggestion, none of the cases on which it relies holds that the requisite permission must come from the system owner and not a legitimate account holder.[6]

---

[6] The Tenth Circuit case the majority cites, *United States* v. *Willis*, 476 F.3d 1121 (10th Cir. 2007), has nothing to do with the meaning of "without authorization." In fact, Willis did "not contest that he provided * * * unauthorized access" to the

At worst, the text of the statute is ambiguous as to who may give authorization. The First Circuit concluded that the meaning of the term "without authorization" in the CFAA "has proven to be elusive," *EF Cultural Travel BV* v. *Explorica*, *Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001), and an unambiguous definition eludes the majority even now. In that circumstance, the rule of lenity requires us to adopt the narrower construction – exactly the construction that is appropriate in light of the CFAA's anti-hacking purpose and concern for the statute's effect on the innocent behavior of millions of citizens. The text provides no refuge for the majority.

As the Supreme Court has repeatedly held, "where there is ambiguity in a criminal statute, doubts are resolved in favor of the defendant." *United States* v. *Bass*, 404 U.S. 336, 348 (1971); *see also United States* v. *Santos*, 553 U.S. 507, 514 (2008) ("The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them."). If a "choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Jones* v. *United States*, 529 U.S. 848, 858 (2000) (quoting *United States* v. *Universal C.I.T. Credit Corp.*, 344 U.S. 218, 221-22 (1952)) (internal quotation marks omitted). We are therefore bound to adopt the construction of CFAA that criminalizes access only by those without permission from *either* an account

---

website at issue. "He merely argue[d] that he had no intent to defraud in so doing. . ." *Id.* at 1126.

holder *or* the system owner. *See also, e.g.*, *Nosal I*, 676 F.3d at 863 (applying the rule of lenity to the CFAA); *Valle*, 807 F.3d at 527 (same); *Miller*, 687 F.3d at 204 (same).

The "venerable" rule of lenity ensures that individuals are on notice when they act. *Santos*, 553 U.S. at 514. It "vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain. * * *" *Id*. We must, therefore, read the CFAA not just in the harsh light of the courtroom but also from the perspective of its potential violators.[7] In the everyday situation that should concern us all, a friend or colleague accessing an account with a shared password would most certainly believe – and with good reason – that his access had been "authorized" by the account holder who shared his password with him. Such a person, accessing an account with the express authorization of its holder, would believe that he was acting not

[7] *Moskal* v. *United States*, 498 U.S. 103 (1990), relied on by the majority for the claim that "the rule of lenity is not triggered [simply] because it is 'possible to articulate' a narrower construction of the statute," is fully consistent with my reading. Here, the narrower reading rises above the possible and even the plausible: it is the natural reading from the perspective of a number of the law's potential violators. Moreover, because the narrower interpretation better harmonizes with the anti-hacking purpose of the CFAA, the ambiguity here is exactly the kind *Moskal* said *does* trigger the rule of lenity: "reasonable doubt persists about [the] statute's intended scope even *after* resort to 'the language and structure, legislative history, and motivating policies' of the statute." *Moskal* v. *United States*, 498 U.S. 103, 108 (1990) (citing *Bifulco* v. *United States*, 447 U.S. 381, 387 (1980)).

just lawfully but ethically.[8] "It's very common for people to let close friends and relatives check their email or access their online accounts," we said in *Nosal I*. "Some may be aware that, if discovered, they may suffer a rebuke from the ISP or a loss of access, but few imagine they might be marched off to federal prison for doing so." 676 F.3d at 861. The majority's construction thus conflicts with the natural interpretation its freshly minted CFAA violators would have given to "without authorization." That alone should defeat the majority's conclusion.

Worse, however, the majority's construction would base criminal liability on system owners' access policies. That is exactly what we rejected in *Nosal I*. *See* 676 F.3d at 860. Precisely because it is unacceptable in our legal system to impose criminal liability on actions that are not proscribed "plainly and unmistakably," *Bass*, 404 U.S. at 348-49, it is also unacceptable to base "criminal liability on violations of private computer use policies." *Nosal I*, 676 F.3d at 860. Not only are those policies "lengthy, opaque, subject to change and seldom read," *id.* at 860, they are also private – by definition not addressed and perhaps not even accessible to shared password recipients who are not official users themselves. Just as the rule of lenity ensures that Congress, not the judiciary, creates federal crimes, *Bass*, 404 U.S. at 348, the rule also ensures that the

[8] It is evident that Nosal is not such a person. This case, however, differs from *Bush* v. *Gore*, 531 U.S. 98 (2000). It is not "a ticket for one train only." Linda Greenhouse, *Thinking About The Supreme Court After* Bush v. Gore, 35 Ind. L. Rev. 435, 436 (2002). The majority's opinion criminalizes the conduct of all the friends and colleagues mentioned above.

clear (and public) words of Congress – not the obscure policies of system owners – delimit their scope.

If this were a civil statute, it might be possible to agree with the majority, but it is not. The plain fact is that the Act unquestionably supports a narrower interpretation than the majority would afford it. Moreover, the CFAA is not the only criminal law that governs computer crime. All fifty states have enacted laws prohibiting computer trespassing. A conclusion that Nosal's actions do not run afoul of the CFAA need not mean that Nosal is free from criminal liability, and adopting the proper construction of the statute need not thwart society's ability to deter computer crime and punish computer criminals – even the "industrious hackers" and "bank robbers" that so alarm the majority.[9]

IV.

In construing any statute, we must be wary of the risks of "selective or arbitrary enforcement." *United*

---

[9] In fact, the ubiquity of state regulation targeting computer trespassing counsels in favor of the narrower interpretation of the federal statute. "Congress has traditionally been reluctant to define as a federal crime conduct readily denounced as criminal by the States." *Bond* v. *United States*, 134 S. Ct. 2077, 2093 (2014) (quoting Bass, 404 U.S. at 349). As such, "we will not be quick to assume that Congress has meant to effect a significant change in the sensitive relation between federal and state criminal jurisdiction." *Id.* at 2089. Because the states are already regulating such conduct, we deemed it appropriate in *Nosal I* to presume that "Congress act[ed] interstitially" in passing the CFAA. We therefore refused to adopt a broader interpretation of the Act in the absence of a clear indication from Congress that such a reading was warranted. 676 F.3d at 857. The same is as true of *Nosal II* as of *Nosal I*.

States v. *Kozminski*, 487 U.S. 931, 952 (1988). The majority's construction of the CFAA threatens exactly that. It criminalizes a broad category of common actions that nobody would expect to be federal crimes. Looking at the fallout from the majority opinion, it is clear that the decision will have "far-reaching effects unintended by Congress." *See Miller*, 687 F.3d at 206 (rejecting a broad interpretation of the CFAA producing such unintended effects).

Simply put, the majority opinion contains no limiting principle.[10] Although the majority disavows the effects of its decision aside from dealing with former employees, it may not by fiat order that the reasoning of its decision stop, like politics used to, "at the water's edge." The statute says nothing about employment. Similarly, *Nosal I* discussed use restrictions, whether imposed by an employer or a third-party website, all in the same way. It did not even hint that employment was somehow special.[11] 676 F.3d at 860-61.

---

[10] The government has not offered a workable standard for distinguishing Nosal's case from innocuous password sharing either in the context of employment or outside of it. With respect to things like Facebook password sharing, for example, the government gamely states that in other "categories of computer users," aside from employees, defendants *might* be able to claim password sharing gave them authorization even if it was against the policy of the website, but does not offer any line of its own or even a hint as to what in the statute permits such a distinction.

[11] The majority tries to dismiss *Nosal I* as irrelevant because in the end it only interprets "exceeds authorized access." This is wrong for two reasons. First, while *Nosal I*'s holding applies directly only to "exceeds authorized access," its discussion of password sharing affects the meaning of "without

It is impossible to discern from the majority opinion what principle distinguishes authorization in Nosal's case from one in which a bank has clearly told customers that no one but the customer may access the customer's account, but a husband nevertheless shares his password with his wife to allow her to pay a bill. So long as the wife knows that the bank does not give her permission to access its servers in any manner, she is in the same position as Nosal and his associates.[12] It is not "advisory" to ask why the majority's opinion does not criminalize this under § 1030(a)(2)(C); yet, the majority suggests no answer to why it does not.

Even if the majority opinion could be limited solely to employment, the consequences would be equally untoward. Very often password sharing between a current and past employee serves the interest of the employer, even if the current employee is technically forbidden by a corporate policy from sharing his

---

authorization" as well. This is because the "close friends [or] relatives" have no right to access Facebook's or the email provider's servers, unless the account holder's password sharing confers such authorization. Although in *Nosal I* we rejected the Seventh Circuit's holding in *Int'l Airport Centers, L.L.C.* v. *Citrin*, that court correctly observed that the distinction between "exceeds authorized access" and "without authorization" is often "paper thin." 440 F.3d 418, 420 (7th Cir. 2006); *see also Miller*, 687 F.3d at 204 (recognizing the "distinction between these terms is arguably minute"). Second, and more important, *Nosal I*'s central message that we must consider the effect of our decision on millions of ordinary citizens applies with equal force to "without authorization" and "exceeds authorized access."

[12] To make the analogy exact, assume the wife had recently closed her account with the bank or withdrawn as a member of a joint-account with her husband and thus had her credentials rescinded.

password. For example, if a current Korn/Ferry employee were looking for a source list for a pitch meeting which his former colleague had created before retirement, he might contact him to ask where the file had been saved. The former employee might say "it's too complicated to explain where it is; send me your password and I'll find it for you." When the current employee complied and the former employee located the file, both would become federal criminals under the majority's opinion. I am confident that such innocuous password sharing among current and former employees is more frequent than the improper password sharing at issue here. Both employees and Congress would be quite surprised to find that the innocent password sharing constitutes criminal conduct under the CFAA.[13]

Brekka, cited repeatedly in the majority opinion, did not threaten to criminalize the everyday conduct of millions of citizens. Nor does that case foreclose the preferable construction of the statute. *Brekka* primarily addressed the question of whether an employee's violation of the duty of loyalty could itself render his access unauthorized. 581 F.3d at 1134-35. Although we found that authorization in that case depended "on actions taken by the employer," that was to distinguish it from plaintiff's claim that authorization "turns on whether the defendant breached a state law duty of loyalty to an employer." *Id.* Brekka's alleged use of an expired log-in

[13] This example also demonstrates the problem with the majority's reliance on the fact that—like all former Korn/Ferry employees—Christian and Jacobson's credentials had expired. The expiration of someone's credentials is not a reliable indicator of criminal culpability in a password sharing case.

presented a very different situation. Brekka had no possible source of authorization, and acted without having permission from *either* an authorized user *or* the system owner. We therefore had no cause to consider whether authorization from a current employee for the use of his password (i.e. password sharing) would constitute "authorization" under the Act. Moreover, it is far less common for people to use an expired or rescinded log-in innocuously than to share passwords contrary to the rules promulgated by employers or website operators. Thus, unlike this case, *Brekka* did not place ordinary citizens in jeopardy for their everyday conduct. That difference alone is dispositive in light of *Nosal I*.

In sum, § 1030(a)(2)(C) covers so large a swath of our daily lives that the majority's construction will "criminalize a broad range of day-to-day activity." *Kozminski*, 487 U.S. at 949. Such "[u]biquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement." *Nosal I*, 676 F.3d at 861.

V.

Nosal's case illustrates some of the special dangers inherent in criminal laws which are frequently violated in the commercial world, yet seldom enforced. To quote a recent comment by a justice of the Supreme Court with regard to a statute that similarly could be used to punish indiscriminately: "It puts at risk behavior that is common. That is a recipe for giving the Justice Department and prosecutors enormous power over [individuals]." Transcript of Oral Argument at 38, *McDonnell* v. *United States*, 136 S. Ct. 891 (2016) (No. 15-474)

(Breyer, J.). Indeed, as this opinion is being filed, the Supreme Court has issued its decision in *McDonnell* and reiterated that "we cannot construe a criminal statute on the assumption that the Government will use it responsibly." *McDonnell* v. *United States*, 579 U.S. __ (June 27, 2016) (citation omitted). Here it is far worse. Broadly interpreted, the CFAA is a recipe for giving large corporations undue power over their rivals, their employees, and ordinary citizens, as well as affording such indiscriminate power to the Justice Department, should we have a president or attorney general who desires to do so.

Nosal was a senior member of Korn/Ferry and intended to start a competing business. He was also due a million dollars from Korn/Ferry if he abided by his departure agreement. When Korn/Ferry began its investigation of Nosal's possible malfeasance, it brought on ex-FBI agents to search through Christian's garbage and follow Jacobson around. It also hired a leading international corporate law firm consisting of over 600 lawyers, O'Melveny and Myers, which charged up to $1,100 per hour for the time of some its partners.[14] One of O'Melveny's lead attorneys had recently left the office of the United States Attorney who would prosecute any case against Nosal. She referred the case to her former colleagues personally. O'Melveny also told the prosecutor that the case was "time-sensitive" because

[14] It was recently reported that more than a few corporate firms, including O'Melveny's rival Gibson, Dunn and Crutcher, charge as much as $2,000 per hour for some partners' time. Natalie Rodriguez, *Meet the $2,000 An Hour Attorney*, Law360, June 11, 2016, http://www.law360.com/articles/804421/meet-the-2-000-an-hour-attorney.

Korn/Ferry would have to file its civil case shortly, but that it would provide the prosecutor with the facts necessary to "demonstrate the criminal culpability of those involved." The law firm also provided the government with the liability theories it believed necessary to convict Nosal under the CFAA. Less than a month after O'Melveny approached the government, the FBI searched the residences of Jacobson, Christian, and the offices of Nosal's new business. That same day Korn/Ferry filed its civil complaint. In total, Korn/Ferry sought almost a million dollars in attorneys' fees from Nosal to compensate it for the work O'Melveny did to "assist" with the criminal prosecution.

To be clear, I am not implying that there is any misconduct on the part of the prosecution in this case. Nevertheless, private assistance of such magnitude blurs the line between criminal and civil law. Courts have long held that "a private citizen lacks a judicially cognizable interest in the prosecution or nonprosecution of another." *Linda R.S.* v. *Richard D.*, 410 U.S. 614, 619 (1973). Korn/Ferry and its counsel's employment of their overwhelming resources to persuade prosecutors to bring charges against an economic competitor has unhealthy ramifications for the legal system. Civil suits ordinarily govern economic controversies. There, private parties may initiate any good-faith action at their own expense. In criminal cases, however, the prosecutor who "seeks truth and not victims, [and] who serves the law and not factional purposes" must decide which cases go forward and which do not. Robert H. Jackson, *The Federal Prosecutor*, Address Before Conference of U.S. Attorneys (April 1, 1940), *in* 24 J. Am. Judicature

Soc'y 18, 20 (1940). These decisions are inevitably affected by a variety of factors including the severity of the crime and the amount of available resources that must be dedicated to a prosecution.

Prosecutors cannot help but be influenced by knowing that they can count on an interested private party to perform and finance much of the work required to convict a business rival. As the Supreme Court found recently: "Prosecutorial discretion involves carefully weighing the benefits of a prosecution against the evidence needed to convict, [and] the resources of the public fisc." *Bond* v. *United States*, 134 S. Ct. 2077, 2093 (2014).[15] The balance weighs differently when a major international corporate firm will bear much of the cost which would otherwise have to be borne by the prosecutor's office. Prosecutors will also be able to use the work product of the country's finest and most highly paid corporate litigators, rather than investing its meager human resources in developing a complex commercial case different in kind from the cases it is ordinarily used to preparing. [16] Undertaking such third-party financed cases which a United States attorney might not have prosecuted

---

[15] Indeed, the Court has recognized that limited government funds sometimes play an important part in restraining potential executive overreach. *See Illinois* v. *Lidster*, 540 U.S. 419, 426 (2004) (finding that limited police resources would be a practical impediment to the "proliferation" of sobriety checkpoints); *see also United States* v. *Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (arguing that technologies like GPS which loosen the check of limited enforcement budgets may necessitate greater judicial oversight).

[16] The fact that the interested party may be able to recover its attorneys' fees if the prosecution is successful does not affect this analysis.

otherwise gives the appearance of well-financed business interests obtaining the services of the prosecutorial branch of government to accomplish their own private purposes, influencing the vast discretion vested in our prosecutors, and causing the enforcement of broad and ill-defined criminal laws seldom enforced except at the behest of those who can afford it. Moreover, to the extent that decisions to pursue such cases are influenced by such extraneous concerns, and prosecutorial discretion is tilted toward their enforcement, other criminal cases that might otherwise be chosen for prosecution may well be neglected and the criminal justice system itself become distorted.

VI.

"There is no doubt that this case is distasteful; it may be far worse than that." *McDonnell* v. *United States,* 579 U.S. __ (June 27, 2016). As the Supreme Court said in *McDonnell*, "our concern is not with tawdry tales of Ferraris, Rolexes, and ball gowns. It is instead with the broader legal implications of the Government's boundless interpretation" of a federal statute. Here, our concern is not with tawdry tales of corporate thievery and executive searches gone wrong. "It is instead with the broader legal implications of the Government's boundless interpretation" of the CFAA. Nosal may have incurred substantial civil liability, and may even be subject to criminal prosecution, but I do not believe he has violated the CFAA, properly construed.[17] I respectfully dissent.

---

[17] Nosal argues that because the jury was instructed under *Pinkerton*, if the conspiracy count and substantive CFAA counts

are vacated or reversed, so too must both the trade secrets counts. The government does not contest this assertion in its answering brief. I would therefore vacate the trade secrets counts. *See United States* v. *Gamboa-Cardenas*, 508 F.3d 491, 502 (9th Cir. 2007) ("Appellees *** did not raise the *** argument in their briefs and thus they have waived it."). For that reason I express no independent view on the trade secrets counts, although I have substantial concerns about the legality of the convictions on those counts as well.

APPENDIX B

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF
CALIFORNIA

No. CR-08-0237 EMC

August 15, 2013

UNITED STATES OF AMERICA

Plaintiff,

v.

DAVID NOSAL,

Defendant.

**ORDER DENYING DEFENDANT'S MOTIONS
(1) FOR A NEW TRIAL AND
(2) FOR ACQUITTAL**

EDWARD M. CHEN, District Judge:

I. INTRODUCTION

Pending before the Court is Defendant's motions for acquittal and for a new trial. Docket Nos. 436, 437. In April 2013, Defendant stood trial on three counts under the Computer Fraud and Abuse Act ("CFAA"), two counts under the Economic Espionage Act ("EEA"), and one count of conspiracy. At the close of evidence, Defendant moved for a directed verdict of acquittal under Rule 29 of the Federal

Rules of Criminal Procedure. Docket No. 397. The Court took the motion under submission and allowed the case to proceed to verdict. Docket No. 398. On April 24, 2013, the jury returned a verdict of guilty on all counts. Docket No. 408. Defendant now brings a motion for acquittal under Rule 29 and for new trial under Rule 33, asserting insufficiency of evidence and legal errors on several points. Docket Nos. 436, 437. As the arguments in the two motions overlap significantly, the Court will consider them together.

II. FACTUAL AND PROCEDURAL HISTORY

The original indictment in this case was filed on April 10, 2008. Docket No. 1. The second superseding indictment ("SSI") was filed on February 28, 2013. Docket No. 309. The government's allegations in the second superseding indictment were as follows.

Defendant is a former high-level employee of Korn/Ferry International ("KFI"), an executive search firm with offices around the world. SSI ¶¶ 1-2. The company is a leading provider of executive recruitment services, assisting companies to fill executive and other high level positions. SSI ¶ 1. Defendant worked for KFI from approximately April 1996 until October 2004. SSI ¶ 2. When he ceased his employment with the firm, he entered into Separation and General Release Agreement, and an Independent Contractor Agreement with KFI. SSI ¶ 2. In these agreements, he agreed to serve as an independent contractor to KFI from November 1, 2004 through October 15, 2005. SSI ¶ 2. He also agreed not to perform executive search or related

services for any other entity during the term of his contract. SSI ¶ 2. In return, he received compensation in the amount of $25,000 per month. SSI ¶ 2. Despite these agreements, Defendant began to set up his own rival executive search firm with the assistance of three other current or former KFI employees: B.C., J.F.L., and M.J. SSI ¶¶ 3-5. J.F.L. was Defendant's assistant while he was a Korn/Ferry employee, and continued to be employed by Korn/Ferry after Defendant's departure. SSI ¶ 4. B.C. was a KFI employee until approximately January 2005. SSI ¶ 3. M.J. was a Korn/Ferry employee until approximately March of 2005. SSI ¶ 5.

The second superseding indictment charges Defendant with three counts of obtaining unauthorized access to a protected computer with intent to defraud and obtaining something of value in violation of the CFAA. SSI ¶ 20-21. The counts are based on three occasions in which J.F.L.'s KFI username and password were used to access KFI's Searcher database. SSI ¶ 20-21. The three incidents took place on April 12, 2005, July 12, 2005, and July 29, 2005. SSI ¶ 21. On each occasion, the person accessing Searcher downloaded information from the database, including source lists of candidates KFI had compiled for previous search assignments. SSI ¶ 21. The government alleges that these searches were performed not by J.F.L., but by B.C. and M.J., neither of whom were KFI employees at the time. SSI ¶ 19.

The second superseding indictment also charges Defendant with unauthorized downloading, copying, and duplicating of trade secrets, as well as

unauthorized receipt and possession of trade secrets, all in violation of the EEA. SSI ¶ 22-24. The indictment does not specifically identify the trade secrets Defendant is alleged to have obtained. As discussed below, however, the government later indicated to Defendant that these charges were based on three specific source lists and one set of information drawn from a source list, all of which B.C. obtained from Searcher and emailed to Defendant.

Finally, Defendant was charged with conspiracy to commit the CFAA and EEA violations. SSI ¶¶ 12-19. Additional facts and a discussion of the evidence produced at trial are included as relevant to the discussion below.

III. DISCUSSION

A. Legal Standard

Under Federal Rule of Criminal Procedure 29, a defendant may file a motion for a judgment of acquittal after a jury verdict. A Rule 29 motion is basically a challenge to the sufficiency of evidence. "In ruling on a Rule 29 motion, 'the relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *United States* v. *Alarcon-Simi*, 300 F.3d 1172, 1176 (9th Cir.2002) (emphasis in original). "[I]t is not the district court's function to determine witness credibility when ruling on a Rule 29 motion." *Id.*

Under Federal Rule of Criminal Procedure 33, a "court may vacate any judgment and grant a new

trial if the interest of justice so requires." Fed.R.Crim.P. 33(a). A motion for a new trial may be granted if an error, "in any reasonable likelihood, [could] have affected the judgment of the jury." *United States* v. *Butler*, 567 F.2d 885, 891 (9th Cir.1978).

The Ninth Circuit has also noted that a motion for a new trial may be granted where there is a sufficiency-of-the evidence problem. As suggested by the language of the rule, where sufficiency of the evidence is at issue,

> [a] district court's power to grant a motion for a new trial is much broader than its power to grant a motion for judgment of acquittal. "The district court need not view the evidence in the light most favorable to the verdict; it may weigh the evidence and in so doing evaluate for itself the credibility of the witnesses." "If the court concludes that, despite the abstract sufficiency of the evidence to sustain the verdict, the evidence preponderates sufficiently heavily against the verdict that *a serious miscarriage of justice may have occurred*, it may set aside the verdict, grant a new trial, and submit the issues for determination by another jury."

United States v. *Alston*, 974 F.2d 1206, 1211-12 (9th Cir.1992) (emphasis added). In short, a motion for a new trial should be granted "only in an exceptional case in which the evidence weighs heavily against the verdict." *United States* v. *Merriweather*, 777 F.2d 503, 507 (9th Cir.1985); *see also United States* v. *Camacho*, 555 F.3d 695, 706 (8th Cir.2009) (stating

that "a new trial motion based on insufficiency of the evidence is to be granted only if the weight of the evidence is heavy enough in favor of acquittal that a guilty verdict may have been a miscarriage of justice[;] [n]ew trial motions based on the weight of the evidence are generally disfavored"); *United States* v. *Martinez*, 763 F.2d 1297, 1312-13 (11th Cir.1985) (stating that "[t]he court may not reweigh the evidence and set aside the verdict simply because it feels some other result would be more reasonable[;] [t]he evidence must preponderate heavily against the verdict, such that it would be a miscarriage of justice to let the verdict stand") (emphasis added).

B. CFAA Counts

Defendant raises a number of arguments as to why he is entitled to either an acquittal or a new trial on the charges under the Computer Fraud and Abuse Act. The CFAA provides criminal penalties for an individual who:

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4). The three CFAA counts are based on three incidents where KFI's Searcher database was accessed using J.F.L.'s password and various information was obtained on April 12, 2005, July 12, 2005, and July 29, 2005, respectively.

Docket No. 309 at 10 (second superseding indictment). Defendant argues that he is entitled to acquittal or new trial on the CFAA counts because (1) no person gained unauthorized access to Searcher within the meaning of the CFAA; (2) the Court's deliberate ignorance instruction was confusing; (3) the government provided insufficient evidence that Defendant had the requisite mental state to commit the CFAA violations because the evidence does not show that he was aware that Searcher was being accessed by someone other than J.F.L.; and (4) there is insufficient evidence of a conspiracy that forms the basis for Defendant's liability on these counts.

1. Unauthorized Access

Defendant argues that he cannot be convicted of the CFAA counts because no person gained "unauthorized access" to Searcher on any of the relevant dates. He advances three basic arguments on this front: (1) that under the Ninth Circuit's *en banc* decision in *United States* v. *Nosal*, 676 F.3d 854 (9th Cir.2012), there can be no CFAA violation where the access was gained with the permission of the password holder and where there was no circumvention of technological barriers; (2) the evidence introduced at trial established that B.C. and M.J. were authorized to access Searcher on the relevant dates; and (3) since Defendant was authorized to receive certain information from Searcher in the course of his work as an independent contractor, he cannot be convicted of accessing a computer without authorization under the CFAA.

a. Circumvention of Technological Barriers

This Court considered and rejected the first argument in denying Defendant's motion to dismiss the remaining CFAA counts on March 12, 2013. Docket No. 314 at 12. The Court noted that, "[n]owhere does the court's opinion in *Nosal* hold that the government is additionally required to allege that a defendant circumvented technological access barriers in bringing charges under § 1030(a)(4)." *Id.* The Court reaffirms its prior ruling. In any event, the Court noted that the indictment does allege circumvention of a technological barrier because "password protection is one of the most obvious technological access barriers that a business could adopt." *Id.*

b. Permission of the Password Holder

Defendant argues that B.C. and M.J. obtained authorization to KFI's Searcher because J.F.L., who had authority, gave them permission, even though (as discussed below), the evidence establishes B.C. and M.J. did not have KFI's authorization. Defendant's argument is without merit. The Court previously rejected this argument, noting that previous Ninth Circuit precedent had made clear "that it is the actions of the *employer* who maintains the computer system that determine whether or not a person is acting with authorization," and that *Nosal* had not altered this rule. *Id.* at 13-14 (emphasis added) (quoting *LVRC Holdings LLC* v. *Brekka*, 581 F.3d 1127, 1135 (9th Cir.2009) ("The plain language of the statute therefore indicates that

'authorization' depends on actions taken by the employer.")). Nothing in the CFAA or cases interpreting it suggests the authorization required under the CFAA can come solely from a password holder even where it contravenes the employer's rule.

At the hearing, Defendant argued that reading the CFAA to proscribe access where the password holder consented to another's use of her password would criminalize the common practice of employees who share passwords with each other in the course of accessing their employer's computer system. In that scenario, however, the co-employees are all authorized to access the computer—even if doing so using a co-worker's password violates the employer's policy. Violating an anti-password swapping policy might violate the employer's rule, but would not entail allowing an unauthorized person access to the employer's computer system in violation of the CFAA. Here, J.F.L. gave her password not to other KFI employees, but to former KFI employees who were *no longer authorized to access KFI's computer system*. The focus, as the *Brekka* court recognized, is on whether an employer authorizes *the person* in question to access the computer. *Brekka*, 581 F.3d at 1133.

c. B.C. and M.J.'s Authorization on the Dates in Question

A reasonable trier of fact could find that B.C. and M.J. were not personally authorized to access Searcher on the relevant dates. The evidence at trial established, as Defendant notes, that B.C. and M.J. were authorized to access Searcher when they worked for KFI, that B.C. worked with Nosal in his

capacity as an independent contractor while she was still a KFI employee, and that while he was an independent contractor KFI contemplated that Defendant could ask a KFI employee for information he needed from Searcher for KFI searches he was conducting. 2 RT 407; 3 RT 474-75; 3 RT 573-74. The evidence at trial, however, also included the following:

- KFI maintained a policy that prohibited employees from sharing passwords. Gov. Ex. 1; 3 RT 563. Before logging in, users saw a screen indicating that they needed "specific authority" to access the KFI computer. Gov. Ex. 5; 3 RT at 565-66.

- Peter Dunn, KFI's general counsel, testified that Defendant's KFI username and password were terminated on December 8, 2004, and that in his opinion, Defendant did not have authorization to access KFI's computer system after that date.[1] 2 RT 421. In November 2004, Defendant asked that he be able to keep his KFI email and voice mail until the end of December, but Dunn denied his request. 2 RT 409-10. At no point thereafter did Defendant ask Dunn to have his KFI username and password reinstated. 2 RT 410.

---

[1] At Defendant's request, the Court provided a limiting instruction at this juncture, stating:

Ladies and gentlemen of the jury, you will be instructed at the end of this case on the term "authorization" and "authorized access." So when witnesses state their opinion, that is their opinion. But it is up to you, ultimately, to apply the law.

2 RT 421.

- Marlene Briski, KFI's Vice President of Information Services, testified that B.C.'s KFI username and password were terminated on January 24, 2005, several days after she stopped working for KFI. 3 RT 573-74. M.J.'s KFI username and password were terminated on March 2, 2005, the day after he stopped working for KFI. 3 RT 574.

- Briski testified that J.F.L. was not authorized to give her KFI computer access credentials to individuals who did not work for KFI. 3 RT 575.

- Dunn testified that Defendant was not authorized to provide access to Searcher to non-KFI employees either during or after his employment with KFI. 3 RT 510-11.

- At no point did Defendant ask Dunn to allow non-KFI employees with whom he was working to have access to KFI's computer system. 2 RT 410. Nor did he tell Dunn that he had KFI employees retrieving information from KFI computers for him, or that B.C. and M.J. had continued to work with Defendant after they left employment with KFI. 2 RT 410-11.

- On April 12, 2005, when B.C. conducted the search that is the basis for the first CFAA count, neither she nor Defendant were KFI employees. 5 RT 959-60. At this point in

time, B.C. testified that all EDS[2] searches that Defendant had been working on as an independent contractor for KFI had been completed and transitioned back to KFI. 5 RT 963. B.C. testified that she did not have permission from KFI to access its computer system on this date. 5 RT 976.

- B.C. testified that at the time of the July 12, 2005 search, which forms the basis for the second CFAA count, she did not have a valid KFI username and password, and that she did not have permission from KFI to access the company's computers. 5 RT 983.

- M.J. testified that at the time of the July 29, 2005 search, which forms the basis for the third CFAA count, he did not have permission from KFI to access the company's computer system. 5 RT 1140, 1143.

Taken together, this evidence is sufficient to establish that neither Defendant nor B.C. nor M.J. had were authorized to access KFI's computers on the relevant dates. A reasonable jury could well have concluded that all three were not authorized, and that B.C. and M.J.'s activities thus constituted unauthorized access in violation of § 1030(a)(4). Nor can it be said that the weight of evidence weighs so heavily against the verdict that a serious miscarriage of justice may have occurred, requiring a new trial.

---

[2] B.C. does not explain what the EDS searches were. Dunn had earlier testified that as an independent contractor, Defendant was charged with completing searches he had begun for four companies: Sinogen, BestBuy, Maxtor, and EDS. 2 RT 419.

There was substantial, indeed, uncontradicted, evidence that neither B.C. nor M.J. had KFI's authorization to access the Searcher database at the time of the events in question. The Court therefore denies both the Rule 29 motion for acquittal and the Rule 33 motion for a new trial on this issue.

d. Nosal's Authorization

Defendant's final argument is that he was authorized to receive certain information from Searcher in the course of his work as an independent contractor, and therefore he cannot be convicted of accessing Searcher without authorization under the CFAA, regardless of who actually accessed the database on his behalf. Docket No. 436 at 14; Docket No. 448 at 4-7. Defendant cites to no authority to support this proposition, other than cases generally discussing the rule of lenity. The text of the statute, however, is concerned not with permission to access *information*, but rather with permission to access a protected *computer*. The provision of the CFAA under which Defendant is charged provides penalties for anyone who:

> knowingly and with intent to defraud, *accesses a protected computer without authorization*, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C.A. § 1030(a)(4) (emphasis added). The statute further defines the term "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." 18 U.S.C.A. § 1030(e)(6) (emphasis added). Cases discussing this provision similarly focus on rights to access a *computer*, not rights to the *information* stored thereon. *See, e.g., Brekka*, 581 F.3d at 1133 (9th Cir.2009) ("It is the employer's decision to allow or to terminate an employee's authorization *to access a computer* that determines whether the employee is with or 'without authorization.' ") (emphasis added). Defendant's argument that since he was authorized to obtain certain information, he cannot be deemed to have violated the CFAA, is thus not supported by the plain text of the statute, and he points to no case so interpreting the CFAA. Nor does Defendant's interpretation of the CFAA make logical sense. Just because a person is authorized generally to receive information from a database does not mean that person can deputize any other person, including one without authorization, to access the computer in clear violation of an employer's rule. The ends do not justify the means.

In any event, in this case, the evidence suggests that Defendant did *not* actually have unqualified access to all of the information on KFI's system. The information Defendant was authorized to receive was limited to information relevant to the searches he was completing for KFI as an independent contractor; however, the information he received was for searches Defendant was conducting for his own business.

2. Deliberate Ignorance Instruction

Defendant contends that he is entitled to a new trial on the CFAA counts because this Court's instruction on deliberate ignorance would have allowed the jury to convict him on the CFAA counts even if they found that J.F.L., who was authorized to access Searcher, had been the one who accessed Searcher. Docket No. 437 at 7-8. The Court's instruction on this front was as follows:

> With respect to Counts 2 through 6 of the indictment (and not Count 1), you may find that the defendant acted knowingly if you find beyond a reasonable doubt that the defendant:
>
> 1. was aware of a high probability that, [B.C., M.J., or J.F.L.] had gained unauthorized access to a computer used in interstate or foreign commerce or communication, or misappropriated trade secrets, downloaded, copied, or duplicated trade secrets without authorization, or received or possessed stolen trade secrets without authorization, and
>
> 2. deliberately avoided learning the truth.
>
> You may not find such knowledge, however, if you find that the defendant actually believed that these individuals had not gained unauthorized access to a computer used in interstate or foreign commerce or communication, or had not misappropriated trade secrets, downloaded, copied, or duplicated trade secrets without authorization, or received or possessed stolen

> trade secrets without authorization, or if you find that the defendant was simply careless. This instruction applies to the terms "knew," "know," or "knowingly," not to the term "firmly believed."

Docket No. 401 at 49. Defendant argues that including the name of J.F.L. who was a KFI employee at all relevant times and was authorized to access the KFI computers, erroneously permitted the jury to convict Defendant even if they found that J.F.L. (not B.C. or M.J.) had been the one who accessed Searcher on the occasions that were the subject of the CFAA counts.

As an initial matter, this is the first time that Defendant has raised this objection. Though Defendant previously objected to this instruction generally, he did not specifically object to the inclusion of J.F.L.'s name in the instruction. Docket No. 334 at 3; 7 RT 1530-33. During a discussion regarding this instruction after the close of the government's case, Defendant objected to a previous version of this instruction, which had not named any individuals, and referred to Defendant's "co-conspirators." 7 RT 1530-33. The government proposed omitting the word "coconspirators," and instead "substituting the actual names of the three people in question." 7 RT 1532-33. Defendant *assented* to this alteration to the instruction. *Id.* Though J.F.L.'s name was not explicitly mentioned, the government specified that it did not intend to include Michael Louie's name in the instruction, and named B.C. and M.J. as two out of the three who would be named in the instruction. *Id.* It was thus quite clear in context that J.F.L. would be the third

person named in the instruction. The Court then issued a version of the jury instructions that included J.F.L.'s name in the deliberate ignorance instruction. Docket No. 400. The following day, Defendant raised additional concerns with the deliberate ignorance instruction, but did not object to the inclusion of J.F.L's name. 8 RT at 1543-46. Hence, Defendant waived any objection to including J.F.L.'s name. Fed. R.Crim. P 30(d) ("A party who objects to any portion of the instructions or to a failure to give a requested instruction must inform the court of the specific objection and the grounds for the objection before the jury retires to deliberate.").

Further, in the context of the entire instruction, the inclusion of J.F.L.'s name in the instruction was not an error. As the instruction applies to both the CFAA and EEA counts, including J.F.L.'s name was appropriate because the government alleged that she had participated in the theft of trade secrets (i.e., the EEA counts). Additionally, the instruction makes sufficiently clear to the jury that they could not convict Defendant on the CFAA counts if they concluded that J.F.L. had been the one to access Searcher. Specifically, it allows a finding of deliberate ignorance only where Defendant was aware of a high probability that one of the named individuals obtained "unauthorized access." The Court's instructions elsewhere defined authorized access under the CFAA:

> Whether a person is authorized to access the computers in this case depends on the actions taken by Korn/Ferry to grant or deny permission to that person to use the computer. A person uses a computer "without

> authorization" when the person has not received permission from Korn/Ferry to use the computer for any purpose (such as when a hacker accesses the computer without any permission), or when Korn/Ferry has rescinded permission to use the computer and the person uses the computer anyway.

Docket No. 401 at 36. In light of this instruction, and the fact that the undisputed evidence showed that J.F.L. was an employee with KFI computer access credentials at all relevant times, there is little risk that inclusion of J.F.L.'s name in the deliberate ignorance instruction confused the jury on the CFAA counts. No new trial in "the interest of justice" is warranted. Fed.R.Crim.P. 33(a). The Court therefore denies Defendant's Rule 33 motion on this issue.[3]

3. Defendant's Knowledge of Downloads

Defendant also contends that he is entitled to an acquittal or new trial because there is insufficient evidence that he was aware that the downloads from Searcher were being conducted by B.C. and M.J., rather than J.F.L., who was authorized to access KFI's computer system. Docket No. 10-11, 15-16. The government, however, presented a significant amount of evidence suggesting that Defendant was aware, or at least maintained deliberate ignorance, of the fact that B.C. and M.J. were accessing Searcher without authorization from KFI. The evidence at trial included:

---

[3] Defendant does not appear to raise this issue in his Rule 29 motion. In any case, the issues Defendant raises here would not constitute error under the Rule 29 standard either.

- In the spring of 2004, J.F.L. and B.C. had conversations about the possibility of Defendant leaving KFI. 6 RT 1284-85. B.C. encouraged Defendant to leave KFI, telling him that they could take KFI information with them when they left. *Id.* Defendant's reaction was to say "don't talk about this in front of me. I don't want to hear it. Talk about it amongst yourselves." 6 RT 1285. Defendant did *not* tell them *not* to take KFI data. *Id.*

- At a later date, but before Defendant left KFI, J.F.L., who had been tasked with making copies of candidate resumes, asked Defendant where to save them. 6 RT 1286. Defendant told her to figure it out on her own, but told her to purchase any media she used for storage using his personal credit card rather than his KFI business card. *Id.*

- During the time he worked at KFI, Defendant relied on B.C. to retrieve information for him from Searcher on a daily basis. 5 RT 921.

- B.C. testified that though J.F.L. was Defendant's executive assistant while he worked for KFI and she had a basic familiarity with Searcher, she typically did not pull old source lists for him; B.C. would do that for him. 5 RT 921-22.

- J.F.L. testified that she had never pulled an old source list or run a custom report for source lists, and that she did not know how

to do either of these things. 6 RT 1279-80, 1337.

- Prior to the April 12, 2005 search, Defendant had discussions with B.C. about how to obtain the information necessary for a search for a client he was trying to attract. B.C. testified that Defendant "was very instructive about where to have—what searches that he had done or what searches from the source list that could be retrieved." 5 RT 958-60. She further testified that Defendant "asked—he asked me to use searches that Korn/Ferry had done in their database, to find candidates for him that he could quickly call." 5 RT 959. She testified that Defendant had told her to "Get what you need. Get what I need." 5 RT 971. J.F.L. was involved in some of these conversations. 5 RT 960. B.C. testified that she subsequently accessed Searcher with J.F.L.'s password and then emailed the information she retrieved to Defendant. 5 RT 959-64.

- On the day of the July 12, 2005 search, B.C. was working in the Nosal Partner's office, and Defendant had been yelling at B.C., telling her that he needed a contact number for a candidate. 5 RT 985, 988. B.C. obtained the number for him from Searcher. 5 RT 988.

- B.C. and Defendant had a romantic as well as professional relationship. 5 RT 925-26. During the course of their romantic

relationship, which ended in the spring of 2005, Defendant and B.C. spoke every day. 5 RT 926. She discussed with him the things she was doing in her work life, including keeping him up-to-date on searches she was working on for him, telling him which source lists she was looking at, and brainstorming source lists to use in new searches. 5 RT 925-26.

- B.C. testified that there was no doubt in her mind that Defendant knew that she was accessing Searcher after she left KFI, and that he knew she was doing so with J.F.L.'s password. 5 RT 1080-81.

- After the civil litigation between Defendant and KFI commenced, Defendant never spoke to B.C. or expressed anger at her about the fact that she had accessed KFI's computer system after she was no longer a KFI employee. 5 RT 1000.

- M.J. testified that though Defendant had never directed him to take source lists from Searcher, it was his understanding based on conversations he had with Defendant, B.C., and others that one of his tasks for the business Defendant was starting was to bring data from KFI. 5 RT at 1104-05.

- In July of 2005, Defendant, M.J., B.C. and others participated in a training by a software company from which Nosal Partners had purchased a database. 5 RT 1135-36. At this training, M.J. mentioned that he had source lists from Searcher for

import into the new database. 5 RT 1137. Defendant denied to the software company representative that they had the data from Searcher. 6 RT 1176, 1271. Defendant winked at M.J. during this interaction. 6 RT 1176. J.F.L. testified that when M.J. said this, she and Defendant looked at each other "a bit startled that [M.J.] would blurt out something like that." 6 RT 1339.

- M.J. testified that Defendant had this reaction to "various situations over time," and that "he knew we had it but he didn't want to kind of acknowledge it." 6 RT 1175-76.

- Defendant expressed surprise at the amount of data M.J. had, but did not tell him to get rid of the data. 5 RT 1137-38. He told M.J. that he did not want to know about the information M.J. had brought from KFI. 6 RT 1216.

- M.J. testified that there was no doubt in his mind that Defendant was aware that data he had obtained for Nosal Partners was obtained from the Searcher database. 6 RT 1229-30.

The above evidence, taken together, was sufficient to support a finding that Defendant knew that B.C. and M.J. had accessed Searcher without authorization, that he had remained deliberately indifferent to this fact, and/or that he conspired to commit the CFAA violations with which he was charged. The jury heard evidence that Defendant gave B.C. specific directions about information that

he wanted from Searcher, and that he was aware that M.J. had a large amount of data taken from Searcher. Importantly, J.F.L., Defendant's longtime executive assistant, did *not* know how to run the types of searches that were the basis for the CFAA counts here. Further, when Defendant had worked for KFI, it had been *B.C.*, and *not J.F.L.*, who would run these types of searches for him. The jury could reasonably have inferred that Defendant, who had worked with J.F.L. closely, would have been aware that she could not have been running the searches in question, and that the work would have to be done by M.J. and B.C. There was evidence that Defendant specifically directed his requests to B.C. and that there was an implicit understanding that M.J. would obtain information from Searcher for Defendant's new business, and that Defendant knew that B.C, and M.J. did not have authorization to access KFI computers after they ended their employment with KFI.

The jury further heard evidence that at different points in time Defendant had specifically instructed J.F.L, B.C., and M.J. that he did not want to know about data they might take from KFI. J.F.L testified to conversations she and B.C. had with Defendant where he had told them to figure such issues out for themselves, and that he did not want to hear about it. M.J. testified that Defendant had indicated to him that he did not want to know about the data M.J. had taken from Searcher, but that M.J. understood from his interactions with Defendant that it was expected that he would obtain information from Searcher. Both B.C. and M.J. testified that they were certain that Defendant knew

that they had accessed Searcher during the relevant period.

Given this evidence, a reasonable jury could have concluded that the government had proved beyond a reasonable doubt that Defendant knew of, was deliberately indifferent to, and/or had conspired to commit the CFAA violations by having B.C. and M.J. access Searcher without KFI's authorization.

The interests of justice do not require a new trial on these grounds. Nor is there insufficient evidence warranting relief under Rule 29. The Court therefore denies both of Defendant's motions on this issue.

4. Evidence of Conspiracy

Defendant argues that there was not sufficient evidence of a conspiracy to convict him of the CFAA violations based on co-conspirator liability. However, the evidence discussed in the previous section is sufficient to support a finding that he entered into a conspiracy to gain unauthorized access to the Searcher database.

Defendant also argues, without much explanation, that in order to establish co-conspirator liability based on conspiracy to violate the CFAA, the government was required to establish that Defendant, B.C., and M.J. entered into a conspiracy *after* B.C. and M.J. stopped working for KFI. Docket No. 436 at 10. This argument seems based on the premise that since B.C. and M.J. could access Searcher with authorization during their employ with KFI, it was not possible to conspire to violate the CFAA until they were no longer employees. The

fact that a CFAA violation was not possible at the time the conspiracy formed, however, does not mean that Defendant, B.C., and M.J. could not have entered a conspiracy in 2004 to commit CFAA violations at some future point when it was anticipated that B.C. and M.J. would no longer employed by KFI (being employed or working independently with Defendant's new business instead). Moreover, they could have entered a conspiracy at that point in time to KFI's steal trade secrets from Searcher to facilitate the establishment of Defendant's new business. The conspiracy would have encompassed not only violation of the EEA (discussed below), but all reasonably foreseeable crimes committed in furtherance of the conspiracy. *United States* v. *Chong*, 419 F.3d 1076, 1081 (9th Cir.2005) (citing *Pinkerton* v. *United States*, 328 U.S. 640 (1946)). Gaining access to those trade secrets through unauthorized means in violation of the CFAA could well have been found to be acts foreseeably contemplated and hence within the scope of the conspiracy to steal trade secrets. In fact, the jury heard evidence from which it could infer that the parties had entered a conspiracy in mid-2004 to commit violations of the CFAA, the EEA, or both. *See, e.g.*, 6 RT 1284-86 (discussions between Defendant, B.C., and J.F.L. about leaving KFI and taking KFI data; Defendant instructed J.F.L. to use his personal credit card to buy discs for use in copying KFI data).

In any case, the jury also heard ample evidence from which they could infer that the parties had entered a conspiracy to commit the CFAA violations after B.C. and M.J. no longer worked at KFI. *See, e.g.*, 5 RT 958-71 (Defendant's directions to B.C.

related to the April 12, 2005 search); 5 RT 925-26 (Defendant and B.C. had close personal as well as professional relationship and discussed work daily); 5 RT at 1104-05; 6 RT 1175-76 (M.J. understood that Defendant wanted him to bring KFI information to the new business; Defendant indicated he did not want to know the details); 5 RT 1080-81; 6 RT 1229-30 (B.C. and M.J. stated they had no doubt that Defendant was aware of their activities in accessing Searcher).

As the Court finds that there was adequate evidence to support the jury's verdict on the conspiracy count, whether based on activities before or after Defendant, B.C., and M.J. left KFI, Defendant's motions on this issue are denied.

C. EEA Counts

The jury returned a verdict of guilty on two counts under the Economic Espionage Act, for unauthorized downloading, copying, and duplicating of trade secrets without authorization; and for receipt and possession of stolen trade secrets. Docket No. 408. In relevant part, this statute reads:

> Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
>
> (1) ...
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads,

> uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) ...
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a).

Prior to trial, the government had indicated that these counts were not based on the contention that Searcher itself was a trade secret; instead, the government asserted that certain source lists that had been obtained from Searcher were the alleged trade secrets the formed the basis for these counts. See Docket No. 335-1 (November 29, 2012 letter identifying the source lists the government contends were trade secrets, including those that were downloaded using B.C., M.J.'s and J.F.L.'s login credentials at various points in 2004 and 2005). Ultimately, with the government's approval, the Court's instructions at the close of trial specifically identify four potential trade secrets: the three source lists contained in the government's Exhibit 58, or (for the Count Six only) the information regarding CFOs

contained in the government's Exhibit 60. Docket No. 401 at 38-39.

Defendant raises four arguments for why he is entitled to an acquittal or new trial on the EEA counts: (1) the Court erred in instructing the jury that it could find Defendant guilty of conspiracy to commit the EEA violations even if there was in fact no trade secret; (2) there was insufficient evidence that the source lists in question were trade secrets; (3) there was insufficient evidence that Defendant and his co-conspirators knew or believed that the source lists were trade secrets; and (4) there is insufficient evidence that Defendant and his co-conspirators knew or believed that taking the source lists would cause KFI economic harm.

1. Hsu and Requirement of Actual Trade Secret

Defendant argues that he is entitled to a new trial on all counts because this Court instructed the jury that it could find Defendant guilty of conspiracy to misappropriate, receive, possess, and transmit trade secrets even if the source lists were not trade secrets so long as Defendant "firmly believed" that they were. Docket No. 437 at 12-17. Since a finding of conspiracy on this theory could be the basis of Defendant's conviction on all other counts on a theory of co-conspirator liability, Defendant argues that error on this front requires a new trial on all counts. See Docket No. 401 at 33 (*Pinkerton* instruction).

The Court instructed the jury as follows with regards to count one of the indictment and the

allegation that Defendant was part of a conspiracy to commit EEA violations:[4]

> In Count One of the indictment, the defendant is charged with conspiracy to misappropriate, receive, possess, and transmit trade secrets. As with the charges for attempt, in order to prove the defendant's guilt beyond a reasonable doubt on the conspiracy charges, the government need not prove the existence of actual trade secrets and that Defendant knew that the information in question was a trade secret. However, the government must prove that Defendant firmly believed that certain information constituted trade secrets.

Docket No. 401 at 46. This instruction was based on *United States* v. *Hsu*, 155 F.3d 189, 193 (3d Cir.1998) and Ninth Circuit cases finding that legal impossibility is not a defense to the attempt or conspiracy charges. *See United States* v. *Fiander*, 547 F.3d 1036, 1042 (9th Cir.2008) ("we have held that a conspiracy conviction may be sustained even where the goal of the conspiracy is impossible"); *United States* v. *Quijada*, 588 F.2d 1253, 1255 (9th Cir.1978) (holding that impossibility is not a defense to attempt, and that "generally a defendant should be treated in accordance with the facts as he supposed them to be").

"Legal impossibility exists when the intended acts would not constitute a crime under the applicable

---

[4] The conspiracy charge also charged Defendant with conspiracy to violate the CFAA. Defendant's objections to that portion of the conspiracy charge are discussed in the section on the CFAA charges above.

law." *United States* v. *McCormick*, 72 F.3d 1404, 1408 (9th Cir.1995) (distinguishing factual impossibility, which "refers to those situations in which, unknown to the defendant, the consummation of the intended criminal act is physically impossible") (internal citations omitted). In *Hsu*, the defendants were charged with attempt to steal trade secrets and conspiracy to steal trade secrets, and requested discovery that would enable them to prove that the documents they had attempted to obtain did not contain trade secrets. *Id.* at 193. The court ruled, however, that the documents were not relevant to the defendant's defense because legal impossibility is not a defense to either attempt or conspiracy. *Id.* at 203. Here, as in *Hsu*, Defendant argues that he should be able to raise the defense of legal impossibility because the information in question was not a trade secret.[5]

---

[5] As the court in *Hsu* noted, this defense could also arguably be classified as one of factual impossibility. 155 F.3d at 199. The court there observed that "the distinction between factual and legal impossibility is essentially a matter of semantics, for every case of legal impossibility can reasonably be characterized as a factual impossibility." *Id.* The Ninth Circuit has also expressed skepticism about drawing a firm distinction between the legal impossibility and factual impossibility. *United States* v. *Quijada*, 588 F.2d 1253, 1255 (9th Cir.1978) ("Specifically, we eschew any effort to distinguish so-called Legal impossibility from Factual impossibility or to establish any general principles capable of solving most, if not all, instances in which the defense is raised. We can only say that generally a defendant should be treated in accordance with the facts as he supposed them to be."). In any case, it matters little whether Defendant's argument is characterized as raising legal or factual impossibility as a defense, because the Ninth Circuit has also recognized that "[f]actual impossibility is not a defense

Though the Ninth Circuit has not explicitly addressed the defense of legal impossibility in a trade secrets case, other circuits have followed *Hsu* in holding that proof of an actual trade secret is not necessary in order to support a conviction for of conspiracy to steal trade secrets. *See United States* v. *Wen Chyu Liu*, 716 F.3d 159, 170 (5th Cir.2013) ("the relevant inquiry in a conspiracy case, such as this one, is whether the defendant entered into an agreement to steal, copy, or receive information that he believed to be a trade secret"); *United States* v. *Yang*, 281 F.3d 534, 544 (6th Cir. 2002) ("The fact that the information they conspired to obtain was not what they believed it to be does not matter because the objective of the Yangs' agreement was to steal trade secrets, and they took an overt step toward achieving that objective."); *United States* v. *Martin*, 228 F.3d 1, 13 (1st Cir.2000) (rejecting challenge to theft of trade secrets conviction on the ground that the defendant actually received no trade secrets); *see also Fiander*, 547 F.3d at 1042 (citing Yang with approval). This Court earlier rejected Defendant's argument that the reasoning in *Hsu* is not applicable here, and that the government was thus required to prove the existence of an actual trade secret in order to secure a conviction on the conspiracy charge. Docket No. 354 at 47-48; Docket No. 402.

This ruling allowing for a conviction of conspiracy even if the conduct did not constitute a substantive violation of the underlying law is consistent with the Supreme Court's recognition that conspiracies themselves are a distinct evil, independent of

---

to an inchoate offense" such as conspiracy. *United States* v. *Fleming*, 215 F.3d 930, 936 (9th Cir.2000).

whether or not their ends are ever achieved. The Court has recognized that "[i]t is elementary that a conspiracy may exist and be punished whether or not the substantive crime ensues, for the conspiracy is a distinct evil, dangerous to the public, and so punishable in itself." *Salinas* v. *United States*, 522 U.S. 52, 65 (1997). "The conspiracy poses a threat to the public over and above the threat of the substantive crime's commission-both because the combination in crime makes more likely the commission of other crimes' and because it decreases the probability that the individuals involved will depart from their path of criminality." *United States* v. *Jimenez Recio*, 537 U.S. 270, 275 (2003) (internal citations omitted). Even if the source lists had not been trade secrets—and thus the object of the conspiracy had been impossible —Defendant and his co-conspirators could have still acted culpably in conspiring to steal what they firmly believed to be trade secrets.[6]

---

[6] The Court's instruction that Defendant could be convicted on the conspiracy charge based on his "firm belief" that the source lists in question were trade secrets is further supported by the legislative history of the EEA. A statement made by the EEA's bill managers discussed safeguards in the bill that would prevent an overly expansive application of the EEA. The statement indicated that one of these safeguards:

is provided by the bill's use of the term "knowingly." For a person to be prosecuted, the person must know *or have a firm belief* that the information he or she is taking is in fact proprietary. Under theft statutes dealing with tangible property, normally, the thief knows that the object he has stolen is indeed a piece of property that he has no lawful right to convert for his personal use. The same principle applies to this measure—for someone to be convicted under this statute he must be aware or *substantially certain* that he is misappropriating a trade secret (although a defense should

In addition to the fact that Defendant offers no new argument that would justify re-visiting the Court's prior ruling, any instructional error here would be harmless as a practical matter. The possibility that the jury could have found Defendant guilty of conspiracy based merely on his "firm belief" that the source lists were trade secrets is obviated by the fact that the jury found Defendant guilty of the substantive EEA counts.

The Court had instructed the jury that in order to find Defendant guilty on Count Five (an EEA count), the jury had to find that at least one of the source lists identified in the government's Exhibit 58 is in fact a trade secret; the Court also instructed to the jury that in order to find Defendant guilty on Count Six (another EEA count), the jury had to find that at least one of the Exhibit 58 source lists or the information regarding CFOs contained in the government's Exhibit 60 was in fact a trade secret. Docket No. 401 at 38-39. The instructions on both counts indicated that the jury also had to find that Defendant knew (not just firmly believed) that the source list or information was a trade secret. *Id.*

---

succeed if it is proven that he actually believed that the information was not proprietary after taking reasonable steps to warrant such belief). A person who takes a trade secret because of ignorance, mistake or accident cannot be prosecuted under the Act.

142 Cong. Rec. S12213 (daily ed. Oct. 2, 1996) (managers' statement for H.R. 3723, the Economic Espionage Bill) (emphasis added). This suggests a legislative intent which contemplated that a firm belief could be sufficient to support a conviction for violation of the EEA. Allowing conviction for conspiracy to violate the EEA based on mere firm belief, therefore, does not appear to be inconsistent with the Congressional intent as indicated by the passage quoted herein.

Since the jury convicted Defendant on Counts Five and Six, they necessarily found that at least one of the source lists B.C. sent to Defendant in Exhibit 58 was a trade secret, and that Defendant was aware of this fact. This verdict makes it logically impossible that the jury convicted Defendant of conspiracy on a finding that he conspired to misappropriate, receive, possess, and transmit information that he believed to be a trade secret but that was in fact not a trade secret. Defendant suffered no prejudice as a result of the alleged instructional error.

Defendant also argues that the Court's instruction pursuant to Hsu amounts to an impermissible constructive amendment to the indictment. Docket No. 437 at 14-17. This Court previously rejected the Defendant's argument that the challenged conspiracy instruction effected a constructive amendment of the indictment because it allowed the government to secure a conviction based on the theory that he firmly believed the source lists were trade secrets, even if they were not. Docket No. 402. In his Rule 33 motion, Defendant raises a new constructive amendment argument for the first time, arguing that the conspiracy instruction allowed the jury to convict Defendant on the conspiracy charge based on a finding that Searcher was a trade secret. He bases this argument on the fact that the Court did not specifically instruct the jury that they could not base a conspiracy conviction on a finding that Defendant and his co-conspirators conspired to steal Searcher, which they firmly believed to be a trade secret.

Viewed in the context of the other jury instructions, Defendant's argument is unconvincing. The Court's

instruction on the elements of conspiracy required the jury to find that "beginning on a date unknown, and continuing to no later than August 2, 2005, there was an agreement between two or more persons to commit at least one crime as charged in the indictment" in order to convict Defendant on the conspiracy charge. Docket No. 401 at 30. As noted above, the substantive EEA charges specifically identified the source lists and CFO information in government Exhibits 58 and 60 as the alleged trade secrets. Docket No. 401 at 38-39. It did not include Searcher.

In light of these other instructions, the Court finds that the jury was not permitted by the instruction to base a conviction on a finding that Searcher was a trade secret. In any event, given that the conviction on the substantive EEA counts means that the jury necessarily found at least one of the source lists in government's Exhibit 58 to be a trade secret, it is improbable if not logically impossible that the jury convicted Defendant of conspiracy solely on the theory that he and his coconspirators firmly believed Searcher to be a trade secret. The Court therefore denies Defendant's motions on the above grounds.

2. Evidence Source Lists Were Trade Secrets

Defendant argues that he is entitled to an acquittal or new trial on the EEA counts because the government failed to introduce sufficient evidence that the source lists in Exhibit 58 or the CFO information in Exhibit 60 were, in fact, trade secrets. Specifically, he argues that the government failed to prove that the information in question was not

drawn entirely from publically available sources, and that the source lists had not been publically disclosed.[7] The EEA defines trade secret as follows:

> the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from

[7] Defendant also argues that there was insufficient evidence regarding the content of the pre-April 2005 downloads, such that there can be no finding that the information downloaded on those occasions cannot be the basis for the EEA convictions. As the substantive EEA counts specified that the trade secrets in question were the source lists in the government's Exhibit 58 and the source-list derived information in the government's Exhibit 60, this argument only applies to the conspiracy count to the degree that it is based on allegations of conspiracy to violate the EEA rather than CFAA. As discussed in the previous section, however, given the jury's verdict on the substantive EEA claims, they necessarily would have found that at least some of the information in Exhibits 58 and 60 constituted a trade secret, so it is highly improbable that the conspiracy conviction is based solely on other alleged trade secrets.

> not being generally known to, and not being readily ascertainable through proper means by, the public;

18 U.S.C. § 1839(3). The Court's instruction on the definition of trade secrets closely tracked this language. Docket No. 401 at 42.[8] Though Defendant offers various cases discussing the definition of trade secrets, he does not contest the accuracy of the Court's instructions on the definition of trade secrets in the instant motions, only the sufficiency of evidence on this issue. Docket No. 436 at 18-35; Docket No. 448 at 15.

a. Creation of Source Lists

It is true that the evidence at trial suggested that much of the information in Searcher was drawn from publically available sources, and that it was often not possible to determine the origin of any particular information contained in a source list. 2 RT 315-21; 4 RT 815-16; 5 RT 1020-21. Further, there was evidence that when individuals in the executive search industry changed firms, they would at times

---

[8] The Court additionally provided the following instruction on trade secrets:

As members of the jury, it is your responsibility to determine whether something constitutes a trade secret under the test I have just given you. Just because a witness referred to certain information or documents as trade secrets does not mean that they are necessarily trade secrets within the meaning of the statute. Similarly, just because a document refers to information as a trade secret, confidential, or proprietary, does not necessarily make that information a trade secret if it does not otherwise meet the test I have just described to you.

Docket No. 401 at 43.

bring information from their old firm with them to their new firm. 2 RT 318-19, 5 RT 1020-21.

The following evidence was also introduced at trial, however, that would support a finding that the source lists derived from Searcher were compilations of both public and non-public information that had been arranged in ways that provided more information and value than a mere recitation of the publically available information:

- Caroline Nahas, KFI's Southern California Managing Director, testified that source lists were "derived from years of accumulated work that came from private information that individuals shared with us." 2 RT 317. She additionally testified that "Searcher is compiled of information that we have built for decades of – since, you know, I believe, 1995. And it's a very valuable tool to us. And it's like the foundation of our work. It's not the only thing, but it is the foundation that we use on every single search." 2 RT 340-41.

- B.C. testified that she would put information into Searcher from a variety of sources, including the internet, Hoovers, ZoomInfo, OneSource, corporate directories, newspapers, and company websites. Once this information was entered into Searcher, it was unnecessary to return to the original sources. 5 RT 1071-73.

- The source lists often included personal contact information for executives that would not have been publically available.

2 RT 322-23; 5 RT 919-20. This information was highly valuable in conducting searches because it enabled the person conducting the search to more easily and privately contact potential candidates. 4 RT 899; 6 RT 1327.

- The source lists contained in the government's Exhibit 58 contain a number of cell, home, and direct telephone numbers for candidates. Gov. Ex. 58.

- KFI employees would often return to an old source list when working on a new assignment because the old lists were helpful to see work that had previously been done and to identify names that would be appropriate for the new search. 2 RT 296-98; 5 RT 1095.

- Nahas testified that KFI employees would draw on old source lists in building a new source list, but would also supplement with additional research to fill gaps in the list. Larger initial source lists, which could have 600 people or more, would then be whittled down by the employees working on the search who would make determinations of who would be the best fit for the position, and who would also call the individuals directly to gauge interest. 2 RT 299-300.

Additionally, the jury could have inferred that the information contained in the source lists was not entirely public based on the fact that Defendant and his co-conspirators went to significant trouble to retrieve this information from Searcher. If the information was all publically available, it would

make little sense for them to go to such an effort to obtain the information from Searcher.

The above evidence amply supports a finding that the information in Searcher was a compilation that included not just information from public sources, but also information drawn from private sources, and that KFI employees had expended considerable time and judgment in collecting, entering, analyzing, and distilling this information. This is especially true of the source lists compiled from the information in Searcher. KFI employees created source lists in response to searches for individual clients; they contained the list of candidates thought to be the best fit for a specific position with a specific employer. These lists were not merely the result of a mechanical search function, but reflected the judgment and work product of KFI employees experienced in the field of recruiting; the lists were the result of a selective process tailored to the particular circumstances of the search. As such, they had value in future similar searches far beyond an unvetted collection of publically available information. The Court therefore rejects Defendant's argument that the source lists cannot be trade secrets because the government failed to prove that they contained nothing but publically available information.

b. Disclosure to Third Parties

Defendant also argues that the government failed to meet its burden of establishing that the information and source lists in question were trade secrets because the government failed to introduce sufficient evidence to demonstrate that these alleged

trade secrets had not been disclosed to any third parties, such as former KFI clients. In support of his argument, Defendant points to *Ruckelshaus* v. *Monsanto Co.*, 467 U.S. 986 (1984). In that case, the Court held that trade secrets could constitute property protected by the Takings Clause of the Fifth Amendment. *Id.* at 1003-04. In discussing the nature of property rights in trade secrets, the Court noted that

> Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others. Information that is public knowledge or that is generally known in an industry cannot be a trade secret. If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.

Id. at 1002.

Defendant correctly points out that the evidence at trial indicated that KFI would sometimes disclose source lists to clients or potential clients, and that KFI would engage in consulting services for clients in which KFI would disclose certain information from Searcher to the client. 2 RT 447-48; 4 RT 807; 5 RT 1020-22. The government also, however, introduced evidence that would support a conclusion that such disclosure was a relatively rare occurrence and that the alleged trade secrets at issue in this case had not been disclosed to third parties, or had

been disclosed only subject to a confidentiality agreement.

- Nahas testified that clients were generally given information from source lists, but not given the lists themselves. 2 RT 299-301, 312-313.

- Dunn testified that when KFI provided information from Searcher to clients, the practice was to designate the information as confidential and for the client's use only. 2 RT 448-49.

- With regards to the specific source lists in question, Briski testified that they had not been posted on the internet or otherwise released by KFI, and that she was unaware of anyone outside KFI who had come into possession of the source lists. 4 RT 865-67.

- B.C. testified that to her knowledge, Searcher was the only place to obtain the information contained in the three source lists contained in the government's Exhibit 58. 5 RT 977-78. From this, the jury could infer that the lists had not been disclosed to any outside entity; if the lists had been given to KFI clients, B.C. could have obtained the lists by asking the clients for them.

- With respect to the information in the government's Exhibit 60, the jury heard evidence that the source list from which the names were copied came from an open search engagement which had begun only twelve days prior to B.C.'s email sending the

> names to Defendant. 4 RT 765-771. Given the short amount of time this list had been in existence, the jury could have reasonably inferred that it had not been disclosed to any entity outside KFI at the time B.C. obtained the information.

On this record, a reasonable jury could have found that the trade secret status of the source lists at issue was not destroyed by any disclosure to third parties.

c. Reasonable Steps to Protect Searcher

The government introduced significant amounts of evidence tending to show more generally that KFI took reasonable steps to protect Searcher and the source lists drawn from Searcher from public disclosure:

- Nahas testified that to her knowledge, KFI did not permit source lists to be sent outside of the company. 2 RT 298. She also testified that non-KFI employees were not permitted to access Searcher or source lists drawn from Searcher. 2 RT 304.
- Searcher could not be accessed unless the user signed onto KFI's computer system with a KFI username and password, but once in the KFI computer system, no additional password was needed to access Searcher. 5 RT 1023-24.
- M.J. testified that prior to leaving KFI, there was never a time when he provided a source list to a KFI competitor. 5 RT 1095.

- Nahas testified that she never sent a source list to a KFI competitor. 2 RT 346.
- In 2005, the Searcher database was housed on servers at a data center in Burbank, California. Access to the center was restricted to two to three KFI employees and access was controlled by biometric identification. The facility has 24/7 guards and monitoring. 3 RT 583-84.
- Searcher is protected by a firewall and anti-virus software. 3 RT 584-85.
- Briski testified that there are "triggers" built into Searcher that allows KFI to later review the downloading activity of users. 3 RT 615-17. Prior to the incidents that form the basis for the allegations in this case, KFI had never detected incidents where employees downloaded large amounts of data immediately prior to the end of their employment on a scale that M.J., B.C., and Louie did. 3 RT 648-49. This incident prompted KFI to build additional "triggers" into Searcher to better monitor downloads from Searcher. *Id.*
- When users ran a custom report in Searcher, a dialog box would appear that stated in relevant part: "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." Gov. Ex. 2 at 7. When the user exported lists from Searcher to excel, the words "Korn/Ferry Proprietary & Confidential" would appear at the top of the document. Gov. Ex. 2 at 12. *See also*

3 RT 614-15 (Briski's testimony concerning these dialog boxes).

To be sure, there is evidence in the record that KFI did not take every conceivable step to protect Searcher and the source lists:

- There was nothing in the KFI system that prevented users from emailing source lists to people or printing out source lists. 5 RT 1026-27.
- Source lists were not encrypted or protected with separate passwords. 5 RT 1026.
- KFI employees would print out source lists, and take the lists home with them. KFI did not have a procedure in place to prevent employees from taking source lists home. 5 RT 1019-20.
- KFI employees would email source lists to people outside of KFI, including clients. 5 RT 1020.

The statute, however, requires only that the owner of trade secrets take "reasonable" steps to protect the trade secrets, not every conceivable step. See *United States* v. *Hanjuan Jin*, 833 F.Supp.2d 977, 1008 (N.D.Ill.2012) ("Thus, while a trade secret owner need not take 'every conceivable step to protect the property from misappropriation,' H.R.Rep. No. 104-788, at 7, 1996 U.S.C.C.A.N. 4021, 4026, the owner must employ precautionary measures that are reasonable under the circumstances.").

d. Conclusion

The evidence at trial is sufficient to support the jury's verdict. The jury heard evidence that the information in the source lists came from a variety of public and non-public sources, and that KFI had expended considerable time and effort to analyze, distill, and arrange that information in a useful manner for specific positions. The jury also heard evidence that KFI took a number of steps to maintain the secrecy of the information in Searcher and the source lists drawn from Searcher. Finally, there was significant evidence from which it could be inferred that the source lists in question had not been previously disclosed to any entity outside of KFI. The government thus introduced sufficient evidence to support a finding that the source lists were compilations of information that were not generally known or readily ascertainable by the public through proper means. As discussed in Section III.C.3 and III.C.4 below, the government also introduced sufficient evidence to support a finding that the source lists derived economic value from the fact that they were secret because they gave KFI an edge over competitors and allowed them to conduct searches for clients more efficiently, quickly finding candidates who were the best fit. The jury thus could have reasonably found that the government had established beyond a reasonable doubt that the source lists were trade secrets within the meaning of the EEA. *See* 18 U.S.C. § 1839(3).

On this record, Defendant has not established that he is entitled to a judgment of acquittal or a new trial. His motions on this issue are therefore denied.

3. Evidence Conspirators Knew or Believed Source Lists Were Trade Secrets

Defendant argues that he is entitled to an acquittal or new trial because the government failed to introduce sufficient evidence that he and his co-conspirators knew that the source lists that were the subject of the EEA counts were trade secrets. He argues that the government introduced no information regarding the co-conspirator's knowledge that is specific to the alleged trade secrets.

Defendant, however, is incorrect on this point. The government introduced evidence showing both that the co-conspirators were generally aware that KFI considered information obtained from Searcher to be confidential, and that they were aware that the specific source lists and information alleged to be trade secrets in this case were, in fact, trade secrets.

- Defendant, M.J., B.C., and J.F.L. all signed documents titled "Agreement to Protect Confidential Information" during the course of their employment with KFI. Gov. Ex. 7, 12, 14, 16. This agreement defined confidential information to include client lists, client prospects, business development information, source lists, executive lists, and candidate lists, profiles, and reports. *Id.* The agreement stated that the employee agreed to keep the confidential information private and use it only in connection with their work for KFI. *Id.*; 5 RT 1093-94.

- As a Managing Director at KFI, Defendant had sent offer letters to M.J. and J.F.L. that

specified, among other terms, that the employee agreed to keep confidential candidate lists, personal histories or resumes, employment information, business information, customer lists, business secrets, and the firm's list of clients and placement candidates. Gov. Ex. 15, 17.

- Dunn testified that KFI would not have hired Defendant had he not signed the confidentiality agreement, and that Defendant at no point indicated that he disagreed with the agreement. 2 RT 357-60.

- B.C. testified that she understood it to be a violation of this confidentiality agreement to email source lists to competitors, and that she felt her actions in taking information from Searcher for Nosal Partners were wrong because the information belonged to KFI. 5 RT 1076-78.

- The source lists in the government's Exhibit 58 have the words "Korn/Ferry Proprietary & Confidential" at the top of each document. Gov. Ex. 58. After B.C. sent these lists to Defendant, he never mentioned or expressed surprise at the fact that the documents contained this heading. 5 RT 976-77.

- B.C. states that to her knowledge, Searcher was the only place to obtain the information contained in the three source lists contained in the government's Exhibit 58. 5 RT 977-78.

- The CFO information contained in the government's Exhibit 60 does not contain this header because it is merely a list of names and contact information pasted into the body of an email. Gov. Ex. 60. However, B.C. testified that she obtained this information from a KFI source list. 5 RT 964-66.

- Briski testified that the information from the Government's Exhibit 60 was copied and pasted from a then-open KFI search for a company called Sirna Therapeutics. 4 RT 767-69. She came to this conclusion because the names were identical, as were certain typographical irregularities, such as some names being in all capital letters. *Id.*

- The government introduced a copy of the list B.C. sent Defendant in Exhibit 60 that had Defendant's handwriting on it, circling some candidates, crossing out others, adding names, and indicating that he had left a message for some of the candidates. 5 RT 968; Gov. Ex. 63. B.C. later sent an email to a Nosal Partners client, with Defendant's knowledge and consent, suggesting one of the candidates from this list. Gov. Ex. 64; 5 RT 968-70.

There was also evidence presented of the co-conspirator's efforts to keep their activities secret, from which the jury could have inferred that they knew the information they were obtaining was a trade secret:

- For at least some searches she ran, B.C. affirmatively checked a box that prevented Searcher from saving a custom report title, which was otherwise the default setting. 3 RT 614, 630-31.

- M.J. states that he took information from Searcher starting in mid-2004—including candidate resumes, source lists, and experience lists—with the intention of bringing this information to Defendant's new business. 5 RT 1107-08. He stated that he did not tell anyone at KFI that he was taking this information, and that he did not want anyone to know. 5 RT 1109-10. He testified that Defendant set the tone for this atmosphere of secrecy in the first conversation he had with M.J. about the new business, telling M.J. to keep the plans for the new business secret. 5 RT 1110.

- J.F.L. testified that in conversations about taking information from KFI, Defendant had told her and B.C. to work out the details between themselves because he did not want to know about it. 6 RT 1284-86. He did not tell them not to take any KFI information. *Id.*

- On December 15, 2004, Defendant sent J.F.L. an email at her KFI email address indicating that he had secured a client for the new business. Gov. Ex. 50. The email also directed M.J. to take the lead on coordinating with the vendor for the new business' database. J.F.L. responded to him

saying: "David, you sent this to me at my KF email. PLEASE be careful." *Id.*

- On April 27, 2005, J.F.L. emailed two documents to B.C. that contained position specifications she had obtained from KFI's computer system. 6 RT 1329-30. She named these two files "Chocolate Chip Cookie Recipes" and "Invitation to Marcy's Bridal Shower." *Id.*; Gov. Ex. 71. J.F.L. testified that she sent these documents to B.C. at B.C.'s request, and that she gave the documents these names to disguise their true contents. 6 RT 1330.

- In June 2005, an individual using J.F.L.'s access credentials ran a search for human resources candidates meeting certain criteria. 3 RT 644-68; Gov. Ex. 31. This individual named the resulting custom report "choc chip." 3 RT 666. The person then created another custom report titled "CCC" and clicked a box to prevent the custom report from being saved. 3 RT 667. This information was downloaded to an Excel document with the title "choc chip cookie recipes." 3 RT 668. The resulting information was burned to a CD that was titled "choc chip cookies." 3 RT 669. After the information was burned to the CD, the user deleted the data from the Excel document saved on the computer, and instead saved a version of the document with the words "four cups of sugar, two cubes of butter" inserted. 3 RT 669.

Though Defendant presented an alternative explanation for this secretive behavior—that he and his co-conspirators were merely trying to avoid tipping off KFI that he was starting his own business in violation of what he contends was an illegal non-compete covenant—the jury could reasonably have concluded that these actions indicated the co-conspirators knew their actions to be criminal. Indeed, Defendant's argument that the non-compete covenant was illegal and unenforceable (discussed below) would seem to undermine the need for secrecy if that were the only reason: if Defendant was certain that the non-compete covenant was unenforceable, what need would he have to hide his activities?

The jury could have inferred that Defendant and his co-conspirators were aware of the trade secret status of the information in question since, at the time in question, they were all current or former KFI employees. Given Defendant's senior position and length of service with KFI, the jury could reasonably inferred his awareness that source lists and similar information drawn from Searcher were valuable trade secrets belonging to KFI. Similarly, B.C., M.J., and J.F.L. had all worked for KFI, and had used Searcher as part of their employment there. The jury could have inferred that they knew of Searcher's value through the use they had made of it, and were aware of the steps KFI took to keep the material secret because they had been exposed to various policies and restrictions on use during the course of their employment.

Indeed, the government produced evidence at trial that Defendant sought to use the source lists and to gain immediate financial benefit by obtaining them

directly from KFI's computers rather than employing his own work effort to derive his own lists. This evidence underscores the likelihood that he knew what he was obtaining was a trade secret.

Looking at this evidence as a whole, a reasonable jury could have concluded that the government had proved beyond a reasonable doubt that Defendant and his co-conspirators knew that the alleged trade secrets were in fact trade secrets. The Court therefore denies Defendant's motions on this ground.

4. Evidence Conspirators Knew or Believed that Taking Source Lists Would Harm KFI

Defendant argues that he is entitled to acquittal or a new trial because the government failed to introduce sufficient evidence that Defendant and his co-conspirators intended or knew that their actions would injure KFI, as is required by the EEA. 18 U.S.C. § 1832(a). The government did, however, present evidence from which the jury could conclude that Defendant and his co-conspirators knew that taking the source lists in the government's Exhibit 58 or the CFO information in the government's Exhibit 60 would injure KFI. In addition to the evidence discussed above about the value of the information found in Searcher and the derived source lists, the government introduced the following evidence, indicating the value of Searcher, the co-conspirator's awareness of this value, and the fact that KFI could be harmed if information from Searcher fell into the hands of a competitor such as Defendant:

- Nahas testified that the executive search industry is highly competitive. 2 RT 290-92. KFI would put a lot of work and research into attempting to solicit clients. *Id.*

- B.C. similarly testified that in order to solicit clients in a competitive bidding process, it was important to have a lot of information about the company, what it was looking for, and potential candidates. 4 RT 889-91.

- M.J. testified that the executive search industry was competitive, and that information was valuable for soliciting and retaining clients. 6 RT 1200-01.

- Nahas testified that if a KFI competitor had access to one of KFI's source lists on a relevant search, this could give the competitor an advantage because they could obtain information that the would not otherwise have had access to. This would permit them to do a better search and possibly obtain business that they would otherwise have gotten. 2 RT 304-05. She described source lists as "the foundation and the springboard and the running start for an assignment." 2 RT 301.

- B.C. testified that KFI ordinarily wouldn't share information with Searcher with competitors because KFI competed with them for business. 5 RT 916-17. Though she had given information from Searcher to friends outside KFI, she did not recall telling her bosses at KFI that she had done so. *Id.*

- M.J. testified that as a KFI employee, he would frequently return to old source lists, because they were helpful in conducting new searches. 5 RT 1095.

- B.C. testified that she would frequently look to source lists from previous similar searches when beginning a new search. 4 RT 893, 897-98. She testified that it was incredibly important to have the contact information contained in Searcher and the source lists, particularly private cell phone and email information for executives, because executives were more likely to respond and to be able to talk to the KFI employee privately. 4 RT 898- 99

- B.C. testified that during her time working with Nosal at KFI, he would at times direct her to look at a source list from a prior search because he was interested in "leveraging names from prior searches in order to help expedite a current search that he was working on or a search that he wanted—that he was pitching for." 5 RT 920-21. She additionally testified that clients generally wanted searches conducted in an expedient manner. 4 RT 886. Conducting searches quickly made clients happy, and "opens the door to more searches." 5 RT 954.

- The Confidentiality Agreements Defendant and his co-conspirators signed described Searcher and the information contained therein as "extremely valuable assets" that

> were "accorded the legal protection applicable to a company's trade secrets." Gov. Ex. 7, 12, 14, 16.

Additionally, the fact that Defendant and his co-conspirators were starting a business that would *compete* with KFI supports an inference that they knew or intended that their actions would injure KFI. The above evidence suggests that Defendant and his co-conspirators were aware of the value of the information contained in Searcher, and sought it because of the advantage it would give them in conducting searches for the new business. Defendant presumably desired the new business to succeed, and given that the business was a direct competitor of KFI's, this could well result in securing clients who might otherwise have gone to KFI for their executive search needs. The Supreme Court has recognized that the owner of a trade secret is harmed when the trade secret is disclosed to competitors:

> Once the data that constitute a trade secret are disclosed to others, or others are allowed to use those data, the holder of the trade secret has lost his property interest in the data.... The economic value of that property right lies in the competitive advantage over others that [the trade secret owner] enjoys by virtue of its exclusive access to the data, and disclosure or use by others of the data would destroy that competitive edge.

Ruckelshaus, 467 U.S. at 1011-12; *see also id.* at 1011 n.15 ("We emphasize that the value of a trade secret lies in the competitive advantage it gives its

owner over competitors."). While it is not clear that *Ruckelshaus*, which did not consider criminal charges for the theft or misappropriation of trade secrets, establishes that this prong of § 1832 is necessarily met when the defendant works for a competitor, the jury may properly have considered these circumstances as probative to the question of whether Defendant and his co-conspirators knew or intended that their actions would harm KFI.

The government additionally argues that even absent *knowledge* that an offense will injure the owner of the trade secrets, a jury can convict if the government proves beyond a reasonable doubt that the defendant *intended* to injure the owner. *See* 18 U.S.C. § 1832(a). At trial, the government introduced evidence that Defendant was angry with KFI because he had not secured a promotion he desired. 5 RT 928, 950-51. It further introduced evidence suggesting that he harbored resentment against KFI and wanted to make a statement around his departure. 5 RT 1067 (Defendant ghost wrote B.C.'s departure email from KFI "because he was interested in creating kind of a fireball effect from his departure"). From this, a jury could have inferred that Defendant intended to harm KFI.

Taken together, this evidence is sufficient for a reasonable jury to find that Defendant and his co-conspirators knew or intended that their actions in taking the source lists and related information would harm KFI. The Court therefore denies Defendant's motions on this ground.

D. Exclusion of Evidence and Argument Regarding Non-Compete Clause

Defendant argues that he is entitled to a new trial under Rule 33 on all counts because he was prejudiced by the Court's order precluding him from arguing that a non-compete provision in his independent contractor agreement with KFI was illegal under California law. Docket No. 437 at 19-30. In the pre-trial order, this Court granted in part Defendant's motion in limine on this issue, ruling that either party could introduce argument or evidence of a person's subjective beliefs about the validity of the non-compete provision where it was relevant to explain that individual's actions or for some other purpose. Docket No. 352 at 6-8. The Court precluded either party, however, from introducing evidence or argument as to whether the provision was *actually* legal and enforceable because this was irrelevant to the issues in this case. *Id.* at 7.

Furthermore, the Court prohibited the government from arguing that Defendant's breach of any non-compete agreement was probative to his motive or intent to defraud. Both at the beginning of the trial and at the close of evidence, the Court gave the jury the following instruction:

> You have heard testimony from some witnesses that Mr. Nosal entered into a noncompetition covenant with Korn/Ferry when he ceased to be an employee and became an independent contractor. Whether the agreement was legal and enforceable is not relevant to the issues in this case. To the

> extent that any of the witnesses offered opinions to whether the defendant's conduct was a breach of any covenant or agreement with Korn/Ferry, that opinion testimony must be disregarded as irrelevant to the issues you are to decide. Additionally, evidence that Mr. Nosal breached or did not breach this covenant is not relevant to the question of whether he is guilty of the crimes charged in this case.

Docket No. 375 at 20; Docket No. 401 at 23.

In the instant motion, Defendant renews his argument that the non-compete provision was unlawful, and that this fact was relevant to his defense. He further argues that even if the Court's ruling on this point was not in error, he was prejudiced by the way the government presented evidence on the non-compete provision because the government to introduced evidence suggesting that Defendant had acted dishonestly in violating the non-compete provision, and Defendant was not permitted to argue that this provision was unlawful. He argues, in the alternative, that the Court should have precluded all mention of the non-compete provision, as the parties' subjective beliefs about its validity were irrelevant to the charges in this case.

1. Relevance of Non-Compete Provision

Defendant offers no new argument that the legality of the non-compete covenant was relevant to any issue in this case. Defendant contends that "the covenant was relevant and exculpatory, as its illegality explained actions on the part of the defendant that otherwise appeared wrongfully deceitful," and that the KFI's efforts "to limit Nosal's

establishment of a new search business by means of an illegal agreement under threat of denying him a huge balloon payment owed him was relevant to prove the innocence of his efforts to avoid detection of his non-KFI work." Docket No. 437 at 2, 20. To the degree that the relevance of the covenant was to explain Defendant's actions, however, what would be relevant is not the actual legality or illegality of the covenant, but Defendant's subjective belief regarding its legality or illegality. This is exactly what the Court permitted in its pre-trial ruling. Defendant identifies no time at trial where he was prevented from presenting evidence about his beliefs regarding the legality of the contract.[9]

Further, as noted above, to the degree that Defendant believed the non-compete covenant to be unlawful and unenforceable, this provides no explanation as to why he felt the need to keep his actions secret (and so behaved). If Defendant had believed that portion of his agreement with KFI to be unenforceable, he would have little need to keep his

---

[9] Defendant also renews his argument that the non-compete covenant was illegal under California law, and additionally brings the new argument that his agreements with KFI were illegal because they erroneously classified him as an independent contractor rather than an employee. Docket No. 437 at 27-30. As he offers no reason why the legality of the non-compete covenant is relevant to the issues in this case, however, these arguments are irrelevant. Further, the newly raised argument seems to actually undercut Defendant's position that the non-compete covenant was illegal, as there are cases suggesting that an employer may restrict a current employee's ability to compete. *See Fowler* v. *Varian Associates, Inc.*, 196 Cal.App.3d 34, 41, 241 Cal.Rptr. 539 (Ct.App.1987) ("During the term of employment, an employer is entitled to its employees' undivided loyalty.") (internal citation omitted).

actions in setting up a competing business secret. If KFI had attempted to stop him or otherwise enforce the covenant, he simply could have taken the matter to court and secured an order recognizing his right to set up his business without forfeiting the payments he was owed under the independent contractor agreement. Hence, Defendant's assertion of the illegality of the covenant, if anything, tends to undermine his claim that he acted secretly not because he knew he was taking trade secrets, but because of the non-compete covenant.

Defendant argues in the alternative that given the ruling excluding evidence of the noncompete provision's legality or illegality, this Court erred in allowing the government to present evidence and argument about the non-compete covenant at all. He argues: "Having ruled instead that the noncompetition covenants were flatly irrelevant to Nosal's guilt of the charges, the Court provided no persuasive rationale why evidence of those provisions or the parties' beliefs concerning the matter was relevant to the jury's consideration of the charges." Docket No. 437 at 31.

As this Court previously found, information about the non-compete covenant, and KFI's belief that Defendant was in violation of the covenant, is relevant to explain why KFI began its investigation into the activities of Defendant and his co-conspirators. Docket No. 352 at 6-8. In this case, Defendant has argued that KFI had initiated its investigation and cooperated with the prosecution out of improper motive, such as a desire to avoid paying him funds he was owed under the independent contractor agreement. *See, e.g.*, Docket

No. 313 at 4 ("The reason [that KFI did not confront Defendant about B.C. and M.J.' s access to Searcher] became apparent some months later, when KF refused to pay Nosal the more than a million dollars it owed him for past work on the ground that he had violated an agreement not to perform independent searches while working as a KF contractor."). Defendant's cross-examination of some of the government's witnesses attempted to question their motives and thus impeach their credibility on this front. 2 RT 334-36 (cross-examination of Nahas included questions about KFI's financial interest in parallel civil litigation); 2 RT 496-98 (cross-examination of Dunn included questions about KFI's desire to have the federal government initiate criminal proceedings against Defendant and his co-conspirators before the balloon payment under the independent contractor agreement came due, and questions about the civil litigation). Further, in his closing argument, Defendant argued that this case was not actually about violations of the CFAA or the EEA, but that it was

> just an effort by Korn/ Ferry to eliminate David Nosal as a competitor; and it's an effort by Korn/Ferry to avoid paying him the money that they owed, and to try to, by whatever means possible, win their $27 million lawsuit against Mr. Nosal.

8 RT 1665. In this context, the Court found it appropriate to allow the government to introduce evidence of the non-compete covenant and the Sandra Horn email to counter the argument that KFI had initiated its investigation into Defendant out of animus or improper motive. Nothing

Defendant points to in his Rule 33 motion convinces the Court that this ruling was an error.

Defendant cites various cases in support of his argument that allowing evidence on various individuals' beliefs about the non-compete covenant was an error, but these cases are not on point. Docket No. 448 at 37-38. The cases and treatises he cites concern the appropriateness of allowing otherwise inadmissible hearsay evidence to show state of mind or to provide context for admissible evidence. *See* 2 McCormick On Evid. § 249 (7th ed.); Hearsay Handbook 4th § 2:10; *United States* v. *Dean*, 980 F.2d 1286, 1288 (9th Cir.1992) (finding hearsay statement that was relevant to show why an officer was present at a certain location were not admissible where the officer's reason for being at that location were not relevant to any issue in the case); *United States* v. *Makhlouta*, 790 F.2d 1400, 1402 (9th Cir.1986) (hearsay statement offered to show FBI agent's state of mind should have been excluded where agent's state of mind was not relevant to defense of entrapment); *United States* v. *Walker*, 673 F.3d 649, 657 (7th Cir.2012). None of these cases address the use of evidence to provide context as discussed above.

Defendant does not object to the evidence about the non-compete covenant on the hearsay grounds (with perhaps the exception of evidence about the "Sandra Horn" email). Hence, the authorization he cites are inapposite. Further, to the extent that Defendant does raise hearsay objections, the Ninth Circuit has noted that hearsay evidence about a tip that lead to an investigation may be admissible to explain the origin and course of an investigation. *United States*

v. *Noriega-Lopez*, 47 F.3d 1177 (9th Cir.1995) ("Here, the testimony about the tip was not hearsay to the extent that it showed how the investigation began and why the agents went to certain locations."); *United States* v. *Cawley*, 630 F.2d 1345, 1350 (9th Cir.1980) ("However, with a proper instruction, the court may admit such evidence of tips as was admitted here to explain why an officer conducted an investigation as he did.").

As Defendant offers no convincing argument that this Court's rulings on the admissibility of evidence and argument regarding the non-compete covenant was in error, this Court rejects Defendant's motion for a new trial on these grounds.

2. Prejudice from Evidence Presented and Excluded at Trial

Even if this Court's rulings on the admissibility of evidence and argument regarding the noncompete covenant was not an error, Defendant argues that he was unfairly prejudiced by the way the government actually presented such evidence and argument at trial. He points to several points in the trial that he contends were prejudicial:

- The testimony of KFI general counsel Peter Dunn, in which he discussed the terms of the non-compete covenant, 2 RT 387-90, and stated that KFI had not paid Defendant the full amount of money identified in the independent contractor agreement because KFI believed that Defendant had breached

the agreement, 2 RT 443-444.[10] On cross-examination, Defendant elicited from Dunn the fact that Defendant contended in the civil suit between the parties that the non-compete covenant was "void and illegal." 2 RT 465. The Court permitted this testimony over the government's objection. The Court sustained, however, the government's objection to Defendant's question when counsel asked Dunn whether non-compete covenants were not illegal in some states. 2 RT 465-66.[11]

- The introduction of an email from a "Sandra Horn," in which she stated that Defendant was conducting searches for KFI clients, and suggesting that KFI could "save a few dollars on your agreement with him," or that they may wish to sue, but stating that if KFI did not do anything to stop him, they would "look like chumps." Gov. Ex. 20. Defendant also objects to Dunn's testimony regarding same. 2 RT 421-30. Dunn testified that after getting the email from Horn, he began an investigation to determine whether

[10] Dunn did not identify the actions Defendant took that KFI believed to be a breach of the agreement on direct examination.

[11] Defendant also objects to the portion of Dunn's testimony in which he stated that KFI had secured a preliminary injunction in a civil case against Defendant. Docket N. 437 at 24. According to Dunn's testimony, however, this preliminary injunction was aimed at preventing Defendant from disseminating certain information belonging to KFI, but did not restrain him from competing against KFI. 2 RT 439-440. It is thus unclear how this testimony would prejudice Defendant relative to the issue of the non-compete covenant.

Defendant was breaching the non-compete covenant. 2RT 426-27.

- The testimony of B.C. that Defendant had a non-solicitation [sic] agreement with KFI, and that he did not comply with this agreement, 5 RT 940-41, that Defendant had her set up an executive search business in her name through which he worked, *id.*, and that Defendant used an alias during some interactions with clients, which B.C. understood to be because he did not want people to know he was conducting search work in breach of his agreement with KFI. 5 RT at 952-53. Defendant did not object to these portions of B.C.'s testimony at trial.

- The testimony of M.J., in which he testified to his understanding of the terms of the non-compete covenant. 5 RT 1099. Defendant did not object to this testimony at trial.

- The rebuttal portion of the government's closing argument, which suggested that the only explanation for Defendant's secretive behavior was that he was engaging in criminal activity. 8 RT 1689-90.

In addition to the limiting instruction identified above, the Court took the following steps to limit any potential prejudice from this evidence:

- During Dunn's testimony regarding the terms of the non-compete covenant, at Defendant's request, the Court made the following statement to the jury: "I've already instructed the jury that a provision, which I

think we referred to as a noncompetition clause, the validity or enforceability of that is not an issue in this case for you to decide." 2 RT at 389. Defendant did not renew his objection after the Court gave this statement.

- When the government introduced the Sandra Horn email during Dunn's testimony, the Court admonished the jury as follows at Defendant's request: "Ladies and gentlemen, I'm going to admit Exhibit Number 20 into evidence. But I need to explain to you that this exhibit is admitted for the purpose of giving you some understanding as to the witness's knowledge and, perhaps, intent, but not to prove the truth of the matters that are stated in this email." 2 RT 423.

Taken together with evidence Defendant elicited on cross examination and this Court's limiting instructions, it cannot be said that the government's evidence and argument related to the non-compete covenant was so unfairly prejudicial as to require a new trial. The Court therefore denies Defendant's Rule 33 motion on this ground.

IV. CONCLUSION

For the foregoing reasons, this Court finds that Defendant has established neither that he is entitled to a judgment of acquittal under Rule 29, nor that a new trial is required in the interests of justice pursuant to Rule 33. Defendant's motion for a new trial and motion for acquittal are **DENIED**. The Rule 29 motion Defendant made at the close of evidence in this case is likewise **DENIED**.

This order disposes of Docket Nos. 397, 436, and 437.

IT IS SO ORDERED.

APPENDIX C

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF
CALIFORNIA

No. CR-08-0237 EMC

March 12, 2013

UNITED STATES OF AMERICA

Plaintiff,

v.

DAVID NOSAL,

Defendant.

ORDER DENYING DEFENDANT'S MOTION TO DISMISS

EDWARD M. CHEN, District Judge:

I. INTRODUCTION

Pending before the Court is Defendant's motion to dismiss three counts of violating the Computer Fraud and Abuse Act ("CFAA"). Docket No. 274, 276.[1] The superseding indictment in this case included eight counts for violations of the CFAA related to unauthorized access of a computerized

[1] Docket No. 274 is the original version of the motion; Docket No. 276 is an amended motion.

database of his former employer, Korn/Ferry. The indictment also included several counts for misappropriation, theft of trade secrets, and conspiracy that are not the subject of this motion. Judge Patel previously dismissed five of the counts for violations of the CFAA. Docket No. 135. The government appealed the dismissal to the Ninth Circuit. A panel of three judges reversed the dismissal, but upon en banc review, the Ninth Circuit affirmed Judge Patel's opinion. Defendant now argues that the Ninth Circuit's en banc opinion clarified the application of the CFAA in a way that now requires dismissal of the remaining CFAA counts, which were not addressed on the appeal. Since the hearing on this motion, the government has secured a second superseding indictment adding additional factual detail to two of the CFAA counts.[2]

II. FACTUAL & PROCEDURAL BACKGROUND

The original indictment in this case was filed on April 10, 2008. Docket No. 1. The first superseding indictment was filed on June 28, 2008. Docket No. 42. The superseding indictment brings various charges against Defendant, including eight charges of violating the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a), for aiding and abetting his co-conspirators in securing unauthorized access to a protected computer with intent to defraud

[2] The second superseding indictment also renumbers the counts. The counts at issue in this motion, which had been numbers three, eight, and nine, are now counts two, three, and four, respectively. Since this motion pertains to the first superseding indictment, it will refer to the counts as numbered therein.

and obtain something of value. *Id.* ¶ 21 (counts 2-9). The following facts are taken from the first superseding indictment.

Defendant is a former employee of Korn/Ferry, an executive search firm headquartered in Los Angeles with offices in San Francisco and Redwood City, California. Superseding Indictment ("SI") ¶¶ 1-2. The company is a leading provider of executive recruitment services, assisting companies to fill executive and other high level positions. SI ¶ 1. Defendant worked for Korn/Ferry from approximately April 1996 until October 2004. SI ¶ 2. When he ceased his employment with the firm, he entered into Separation and General Release Agreement, and an Independent Contractor Agreement with Korn/Ferry. SI ¶ 2. In these agreements, he agreed to serve as an independent contractor to Korn/Ferry from November 1, 2004 through October 15, 2005. SI ¶ 2. He also agreed not to perform executive search or related services for any other entity during the term of his contract. SI ¶ 2. In return, he received compensation in the amount of $25,000 per month. SI ¶ 2. Despite these agreements, Defendant began to set up his own rival executive search firm with the assistance of three other current or former Korn/Ferry employees, Becky Christian, J.F., and M.J. SI ¶¶ 3-5. J.F. was Defendant's assistant while he was a Korn/Ferry employee, and continued to be employed by Korn/Ferry after Defendant's departure. SI ¶ 4. M.J. was a Korn/Ferry employee until approximately March of 2005. SI ¶ 5.

Christian, who is also named as a defendant in the superseding indictment, was employed by

Korn/Ferry from approximately September 1999 to approximately January 2005. SI ¶ 3. After leaving Korn/Ferry, she set up an executive search firm known as Christian & Associates, though she was in fact working with Defendant to set up his executive search firm. SI ¶ 3. Christian generally retained 20% of the revenues from the searches the two conducted, while Defendant retained 80%. SI ¶ 3.

Korn/Ferry maintained the "Searcher" database, a proprietary database of executives and companies. SI ¶ 6. Using the "Custom Report" feature of the database, Korn/Ferry employees were able to created targeted reports on executives, companies, and prior search engagements Korn/Ferry had conducted for clients. SI ¶ 6. The database was also capable of producing "source lists," or candidate lists, which were provided to client companies with regards to a particular position they were trying to fill. SI ¶ 8. Korn/Ferry had built up the information contained in the Searcher database over many years, and considered it to be one of the most comprehensive databases of its kind in the world. SI ¶ 7.

Korn/Ferry took a number of steps to preserve the confidential nature of the Searcher database, including controlling electronic access to the database, and controlling physical access to the servers on which it was stored. SI ¶ 9. Korn/ Ferry employees received unique user names and passwords that allowed them to access the company's computer systems, including the Searcher Database. SI ¶ 9. These passwords were intended for use by *1055 employees only. SI ¶ 9. All Korn/Ferry employees, including Defendant, entered into agreements explaining the proprietary nature of the

Searcher database, and restricting the use of the database and related information to legitimate company business. SI ¶ 10. Defendant executed such an agreement on or about April 26, 1996. SI ¶ 10.

Korn/Ferry also explicitly noted the confidential and proprietary nature of the information from the Searcher database on reports and in the computer logon process. SI ¶ 11. All custom reports generated from the database had the phrase "Korn/Ferry Proprietary and Confidential" written across the top. SI ¶ 11. When an individual logged on to the Korn/Ferry computer system, the following notification was displayed

> This 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....

SI ¶ 11.

The superseding indictment alleges that Defendant, along with co-conspirator Christian and others, "did steal, and without authorization knowingly take by fraud, artifice, and deception, trade secrets from Korn/Ferry's computer system, including source lists." SI ¶ 15. The indictment alleges that individual co-conspirators and others obtained these source lists and other trade secrets by using their own Korn/Ferry usernames and passwords prior to and upon termination, and that they did so without authorization and in excess of

authorization. SI ¶ 16. Defendant and co-conspirators also obtained trade secrets from Korn/Ferry's computer system by using, either directly or through J.F., J.F.'s Korn/Ferry username and password, and that this was done without authorization and in excess of authorization. SE ¶ 17. The specific factual allegations related to the various CFAA counts in the first superseding indictment are as follows:

A. Count 2

During the fourth quarter of 2004, just prior to the end of her employment with Korn/Ferry, Christian downloaded custom reports from the Searcher database containing over 3000 records. SI ¶ 19j. She took copies of these reports with her when she left the firm. SI ¶ 19j.

B. Count 3

On or about April 11, 2005, Christian sent an email to J.F. that stated in part, "It is to [sic] difficult to explain the searcher run I would need to log in as you." SI ¶ 19a. The next day, Christian emailed Defendant three Korn/Ferry source lists of Chief Financial Officers ("CFOs") that had been downloaded from the Searcher database earlier that day using J.F.'s username and password. SI ¶ 19b. These source lists were marked as proprietary and confidential. SI ¶ 19b. Defendant and Christian later used individuals on this source list in performing a Chief Financial Officer ("CFO") search for Company B. SI ¶ 19e.

The second superseding indictment specifies that it was Christian who downloaded the source lists after

J.F. provided Christian with her password. Second Superseding Indictment ("SSI") ¶ 19a. Christian did not have authorization from Korn/Ferry to access its computer system at that time. *Id.*

C. Count 4

Also in April 2005, Company C retained Defendant to conduct a search for a senior vice president of human resources. SI ¶ 19h. The CEO of Company C emailed Defendant on April 25, 2005, asking Defendant to draft a job description for the position, and requesting that Defendant "make sure that the payment terms are the aggressive ones you quoted." SI ¶ 19h. On April 29, Christian emailed the CEO of Company C a position description, copying Defendant, and signing the email "David & Becky." SI ¶ 19i. This position description was largely identical to a position specification recently obtained from Korn/Ferry's computer system by J.F. SI ¶ 19i.

D. Count 5

On or about May 26, 2005, M.J. contacted J.F., requesting that J.F. obtain information from the Searcher database on 17 individuals, and on a specific prior Korn/Ferry search engagement. SI ¶ 19l. M.J. had obtained the names of at least some of the individuals from Defendant. SI ¶ 19l. J.F. obtained the requested information from the Searcher database, and copied the files containing the information onto a C.D., which J.F. then provided to M.J. SI ¶ 19l. Defendant later used at least some of this information in a meeting with a prospective client. SI ¶ 19l.

E. Count 6

On or about June 3, 2005, J.F. performed a query within the Searcher database for human resources managers at M.J.'s request. SI ¶ 19m. This query yielded a list of approximately 366 executives, which J.F. then exported to a spreadsheet titled "Choc Chip Cookie Recipes," and burned to a C.D. titled "ChocChip Cookies." SI ¶ 19m. J.F. later provided this C.D. to M.J. for use in the search for Company C. SI ¶ 19m.

F. Count 7

On or about June 23, 2005, J.F. used the Searcher database to create a custom report for senior vice president supply chain managers working at various companies. SI ¶ 19n. This report listed approximately 1,205 executives. SI ¶ 19n. J.F. later provided the custom report to Christian, who used it in an executive search. SI ¶ 19n.

G. Count 8

On or about July 12, 2005, an individual used a computer at Defendant's San Francisco offices to remotely log into Korn/Ferry's computer network using J.F.'s username and password. SI ¶ 19f. A co-conspirator then ran queries for information on two of the individuals who were being considered for Company B's CFO position. SI ¶ 19f. The following month, Company B announced that it had hired one of these two individuals. SI ¶ 19f.

The second superseding indictment does not identify who logged onto the computer, but does specify that Christian was the one who ran the

queries, and that she additionally downloaded two source lists from the Korn/Ferry system. SSI ¶ 19f.

H. Count 9

On or about July 29, 2005, J.F. used M.J.'s computer in Defendant's offices to remotely log into the Korn/Ferry computer network with her username and password. SI ¶ 19*o*. She then turned the computer over to M.J., who used the Searcher database to download information from the database to the computer, including 25 source lists. SI ¶ 19o.

I. Relevant Procedural History

On January 12, 2009, Defendant filed a motion to dismiss various counts in the superseding indictment, including the CFAA counts. Docket No. 84. Defendant argued that the CFAA does not cover misuse or misappropriation of information obtained by employees with authorization to access the information, and that the counts should thus be dismissed because the indictment alleges nothing more. *Id.* at 3-7. Judge Patel denied Defendant's motion to dismiss the CFAA counts, holding that the statute covered the situations alleged in the complaint. Docket No. 105.

In September 2009, the Ninth Circuit decided *LVRC Holdings LLC* v. *Brekka*, which interpreted the CFAA's prohibition on accessing computers "without authorization" or "exceeding authorized access." 581 F.3d 1127, 1133-35 (9th Cir.2009). In light of *Brekka*, Defendant filed a renewed motion to dismiss on October 5, 2009. Docket No. 122. Judge Patel granted Defendant's motion as to counts two, and four through seven, those counts which were

predicated on allegations that Christian, J.F., or M.J. accessed Korn/Ferry's computers while they were still employed by Korn/Ferry, and thus still permitted to access the Searcher database. Docket No. 135 at 9.

The government appealed these dismissals to the Ninth Circuit. A three judge panel of the Ninth Circuit reversed, but Defendant successfully sought en banc review, and the en banc panel of the Ninth Circuit upheld the dismissals. *United States* v. *Nosal*, 676 F.3d 854 (9th Cir.2012). Though counts three, eight, and nine were not considered on appeal, Defendant now argues that the Ninth Circuit's decision in *Nosal* requires that those claims be dismissed as well.

III. DISCUSSION

Under Rule 12 of the Federal Rules of Criminal Procedure, a Defendant may make a motion to dismiss before trial raising "any defense, objection, or request that the court can determine without a trial of the general issue." Fed.R.Crim.P. 12(b)(2). In analyzing a motion to dismiss an indictment, the court must accept the truth of the facts alleged in the indictment. *United States* v. *Boren*, 278 F.3d 911, 914 (9th Cir.2002). "An indictment will withstand a motion to dismiss 'if it contains the elements of the charged offense in sufficient detail (1) to enable the defendant to prepare his defense; (2) to ensure him that he is being prosecuted on the basis of the facts presented to the grand jury; (3) to enable him to plead double jeopardy; and (4) to inform the court of the alleged facts so that it can determine the sufficiency of the charge.' " *United States* v. *Rosi*,

27 F.3d 409, 414 (9th Cir.1994) (quoting *United States* v. *Bernhardt*, 840 F.2d 1441, 1445 (9th Cir.1988)).

An indictment will be found defective and dismissed if it fails to recite an essential element of the charged offence. *United States* v. *Godinez-Rabadan*, 289 F.3d 630, 632 (9th Cir.2002). The Supreme Court has held that "[i]t is generally sufficient that an indictment set forth the offense in the words of the statute itself, as long as those words of themselves fully, directly, and expressly, without any uncertainty or ambiguity, set forth all the elements necessary to constitute the offence intended to be punished." *Hamling* v. *United States*, 418 U.S. 87, 117, 94, 94 S.Ct. 2887, 41 L.Ed.2d 590 (1974) (internal citations and quotation marks omitted). The Ninth Circuit has noted, however, that "implied, necessary elements, not present in the statutory language, must be included in an indictment." *United States* v. *Jackson*, 72 F.3d 1370, 1380 (9th Cir.1995). On the other hand, indictments are not required to incorporate judicial decisions that have interpreted the statutory language. *United States* v. *Renteria*, 557 F.3d 1003, 1006-07 (9th Cir.2009).

A. CFAA Statutory Language

The CFAA provides criminal penalties for an individual who:

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only

> of the use of the computer and the value of such use is not more than $5,000 in any 1-year period

18 U.S.C. § 1030(a)(4). In order to establish a violation of this provision, the government must show that Defendant "(1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further [ed] the intended fraud and obtain[ed] anything of value." *Brekka*, 581 F.3d at 1132. The statute does not define the term "authorization," but does define the phrase "exceeds authorized access" as meaning "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." *Id.* § 1030(e)(6).

Judge Patel initially denied Defendant's motion to dismiss the CFAA counts under this provision. Docket No. 105. Judge Patel recognized that the Ninth Circuit had not yet addressed whether the CFAA applied to a user who was otherwise authorized to access a computer but who did so with the intent to misuse or misappropriate information. *Id.* at 6. Surveying cases from other circuits, however, she concluded that "A CFAA violation under section 1030(a)(4) occurs when a person accesses a protected computer knowingly and with the intent to defraud—which renders the access unauthorized or in excess of authorization—and then, by means of such conduct, the person furthers the intended fraud." *Id.* at 8. As Defendant and his co-conspirators had accessed the Searcher database with the intent to make unauthorized use of the

information therein, Judge Patel found that they were thus acting without authorization or in excess of authorized access. *Id.* at 9-10.

B. *LVRC Holdings* v. *Brekka*

Shortly thereafter, the Ninth Circuit considered the interpretation of the term "without authorization" under the CFAA in *Brekka*. 581 F.3d at 1133-35. In that case, which arose under the provision of the CFAA that allows a private right of action for anyone who suffers damage from violations of one of the criminal provisions of that Act, an employer sued a former employee who had allegedly acted without authorization in emailing certain work files to his personal computer. *Id.* at 1129-30. At the time the defendant emailed himself the files, he was an employee with authorization to access the files in question in the course of performing his duties. *Id.* The employer argued, however, that he had violated the CFAA because he accessed and transmitted the files not for the purposes of executing his duties, but to further his own personal interests. *Id.* at 1132.

The court rejected this argument, and held that whether an employee using an employer's computer is acting with authorization depends not on the user's intent, but on the employer's actions to grant or deny permission to use the computer or relevant content. *Id.* at 1135. The court held that the prohibition on accessing a computer "without authorization" referred to one who "accesses a computer without any permission at all, while a person who 'exceeds authorized access,' has permission to access the computer, but accesses information on the computer that the person is not

entitled to access." *Id.* at 1133. Based on this interpretation of the statute, the court concluded that the defendant had not acted either without authorization or in excess of his authorization because he had possessed authorization to access the relevant files at the time that he emailed them, and his motivation for doing so did not render his access "without authorization." *Id.* at 1135.

Following *Brekka*, Judge Patel reconsidered the earlier ruling denying Defendant's motion to dismiss the CFAA claims. Docket No. 135. In her January 6, 2010 order, 2010 WL 934257, she noted that reading *Brekka* together with the statutory definition of "exceeds authorized access" makes clear that, "an individual's intent in accessing a computer, be it to defraud or otherwise, is irrelevant in determining whether an individual has permission or is authorized to access the computer." *Id.* at *8. As counts two and four through seven were based on allegations that Christian and J.F. had accessed the Searcher database during their employment with Korn/Ferry, and thus during a period where they were authorized to access the database, Judge Patel found that they had not acted without authorization or in excess of authorization. *Id.* at *11. Accordingly, those claims were dismissed. *Id.*

Considering the remaining counts under the CFAA, Judge Patel noted that on its face, the indictment did not explicitly specify who accessed the Searcher database in the incidents that are the basis for counts three and eight. *Id.* at *12; *see* SI ¶¶ 19b, 19f, 21. At the December 16, 2009 hearing on the motion to reconsider, the government indicated that at trial it intends to introduce evidence that it was Christian

who accessed the database on those occasions. Docket No. 135 at 12; Def.'s Opp. at 3. In light of this disclosure, Judge Patel declined to dismiss those counts. Docket No. 135. at 12. As noted above, the second superseding indictment amends these counts to include allegations that Christian accessed the database on those occasions. SSI ¶ 19. As to count nine, Judge Patel noted that the indictment specifically alleged that J.F. had logged onto the database and then turned over access to M.J., who was then no longer a Korn/Ferry employee. *Id.* at 12-13; SI ¶¶ 19*o*, 21. As this count specifically alleged database access by an individual without authorization, Judge Patel denied the motion to dismiss this count. Docket No. 135 at 13.

C. The Ninth Circuit's Decision in *Nosal*

The government appealed the dismissal of counts two and four through seven. On appeal, the Ninth Circuit sitting en banc rejected the government's argument that this case is distinguishable from *Brekka* because Korn/Ferry had an explicit policy forbidding use of the contents of the Searcher database for purposes other than performing one's duties as a Korn/Ferry employee. 676 F.3d at 857-58. The court held "that 'exceeds authorized access' in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use." *Id.* at 863-64. In so holding, the court expressed concern that interpreting the CFAA to create criminal penalties for violations of use agreements "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* at 857. The court thus rejected the argument that an individual could

be liable for accessing a computer in excess of authorization when they had permission to access the information on a computer, but did so for a purpose not condoned by the relevant use agreement. *Id.*

The court noted that a related provision of the CFAA provided criminal penalties for exceeding authorized access of a computer even without any culpable intent. *Id.* at 859. Allowing a definition of "exceeds authorized access" that includes actions that violate use agreements (as opposed to access restrictions) would create sweeping criminal liability for users of the numerous websites and computer systems that have lengthy use agreements that often go unread by users. *Id.* at 860-62. Since the court found that the plain language of the CFAA did not clearly create liability for violations of use agreements, the rule of lenity precluded interpreting the law in such a way that would create such sweeping liability. *Id.* at 863. Rather, a violation of the CFAA requires unauthorized access (or access that exceeds authorization), not misuse of information after obtaining authorized access. The court noted that the narrower interpretation of the phrase "exceeds authorized access" is more consistent with the text of the statute, the legislative history, and the purpose of the CFAA. *Id.* at 863-64.

D. Application to Remaining CFAA Counts

1. Defendant's Definition of Hacking

Defendant now argues that the Ninth Circuit's opinion in *Nosal* limits the applicability of the CFAA to not just unauthorized access but to hacking crimes where the defendant circumvented technological

barriers to access a computer. Thus, Defendant argues, the remaining CFAA claims must be dismissed because they do not include allegations that Defendant or his co-conspirators circumvented any technological access barriers.

The Ninth Circuit acknowledged that the CFAA was passed "primarily to address the growing problem of computer hacking." *Id.* at 858. The court further rejected the government's argument that accessing a computer "without authorization" was intended to refer to hackers, while accessing a computer in a way that "exceeds authorized access" necessarily refers to authorized users who access a computer for an unauthorized purpose.

> it is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.

Id. at 858 (emphasis in original). The court noted that the Defendant's "narrower interpretation [of the CFAA] is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation

of trade secrets—a subject Congress has dealt with elsewhere." *Id.* at 863.

The court did not, however, explicitly hold that the CFAA is limited to hacking crimes, or discuss the implications of so limiting the statute. For example, the court did not revisit the elements of crimes under § 1030(a)(4) as articulated in *Brekka*, where it held the elements of a violation of that provision were: (1) accessing a protected computer; (2) without authorization or exceeding such authorization that was granted; (3) knowingly and with intent to defraud; and thereby (4) furthering the intended fraud and obtaining anything of value. *Brekka*, 581 F.3d at 1132. Nowhere does the court's opinion in *Nosal* hold that the government is additionally required to allege that a defendant circumvented technological access barriers in bringing charges under § 1030(a)(4). Instead, *Nosal* holds only that it is not a violation of the CFAA to access a computer with permission, but with the intent to use the information gained thereby in violation of a use agreement. 676 F.3d at 863-64. The court did not address limits on liability under the CFAA based on the *manner* in which access is limited, whether by technological barrier or otherwise. *Id.* Thus, Defendant's interpretation is not a fair reading of *Nosal* on this front is simply incorrect. Hacking was only a shorthand term used as common parlance by the court to describe the general purpose of the CFAA, and its use of the phase "circumvention of technological access barriers" was an aside that does not appear to have been intended as having some precise definitional force.

Even if *Nosal* added a "circumventing technological access barriers" element to crimes under § 1030(a)(4), the indictment sufficiently alleges such circumvention. As the government points out "password protection is one of the most obvious technological access barriers that a business could adopt." Gov.'s Opp. at 1. Faced with this reality, Defendant acknowledges that the Ninth Circuit did not offer a definition of hacking, and urges this Court to look to the definition in the Digital Millenium Copyright Act, which provides that to " 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). However, there is no legal basis to incorporate into the CFAA the Digital Millenium Copyright Act which was passed 14 years after the CFAA and which concerned matters separate and distinct from the CFAA.[3] Moreover, it is noteworthy that neither the CFAA nor the Digital Millenium Copyright Act employs the term "hacking." In any event, even if the Digital Millenium Copyright Act's definition of "circumvent a technological measure" were to inform the scope of the CFAA, as noted above, the actions alleged in the indictment fall within it. Use of another's password "avoids" and

[3] The CFAA is aimed at addressing various forms of computer-related crime, such as hacking. *See Nosal*, 676 F.3d at 858. The Digital Millenium Copyright Act creates various criminal and civil penalties for circumventing copyright protection systems, including the circumvention of technological measures intended to protect copyrighted materials. 17 U.S.C. § 1201-1204.

"bypasses" the technological measure of password protection.

Defendant argues that the remaining CFAA claims fail because they do not allege "J.F.'s password was obtained illegally or without her consent." Def.'s Mot. at 5. Defendant's argument is premised in part on the notion that because J.F. allowed Defendant's co-conspirators to use her credentials to access the Korn/Ferry system, the co-conspirators cannot be said to be acting "without authorization" in accessing the Searcher database. In *Brekka*, however, the Ninth Circuit made clear that it is the actions of the employer who maintains the computer system that determine whether or not a person is acting with authorization. *Brekka*, 581 F.3d at 1135 ("The plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer."). Further, the CFAA appears to contemplate that one using the password of another may be accessing a computer without authorization, as it elsewhere provides penalties for anyone who "knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization." 18 U.S.C. § 1030(a)(6).[4]

---

[4] In support of his argument that there is no criminal liability under the CFAA because J.F. willingly provided her access credentials, Defendant cites to an example given by the court in *Nosal*, where the court, discussing the variety of terms to be found in use restrictions, notes that Facebook's user agreement makes it a violation of terms to allow another person to log into your account. *Nosal*, 676 F.3d at 861. Besides constituting a mere example cited in dicta, that situation is distinguishable from the circumstances here. First, in the case of Facebook, what is at issue is a use restriction that restricts a user from

Additionally, Defendant argues that the CFAA does not cover situations where an employee voluntarily provides her password to another by analogizing to the law of trespass with regards to physical property: "Just as consensual use of an employee's key to gain physical access is not trespass, consensual use of an employee's computer password is not hacking." Def.'s Mot. at 6. Defendant argues that the court in *Nosal* held that "the CFAA was based on principles of trespass." *Id.* This is a mischaracterization of the opinion in Nosal, which merely noted that the CFAA was passed to address the growing problem of hacking, and quoted a Senate report that stated "[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system." *Nosal*, 676 F.3d at 858 (quoting S.Rep. No. 99-432, at 9 (1986), 1986 U.S.C.C.A.N. 2479, 2487 (Conf.Rep.)). Aside from these passing comments positing an analogy, Defendant points to nothing in the wording of the CFAA or interpretive case law to support its construction. If the CFAA were not to apply where an authorized employee gave or even sold his or her password to another unauthorized individual, the CFAA could be rendered toothless. Surely, Congress could not have intended such a result.

---

giving their password to another person. Furthermore, allowing such person to use one's password permits them to access the user's Facebook account containing the user's personal account and information; it does not allow access to any Facebook trade secrets. In the case at bar, what is being accessed by circumventing the password protection is Korn/Ferry's trade secrets.

2. "Access"

The factual scenario presented in count nine, does, however, raises the question of how to interpret the term "access" in the CFAA. Defendant argues that J.F. was the individual "accessing" the Korn/Ferry system when she logged in using her password, and that M.J.'s use of the system *after* the login does not constitute unauthorized "access" within the meaning of the statute. The government, on the other hand, argues that "access" encompasses ongoing use, including M.J.'s unauthorized use of the system after J.F. logged in.

In support of its argument, the government cites to two Senate Reports from the CFAA's legislative history. The first, from the 1996 amendments to the CFAA, notes that "the term 'obtaining information' includes merely reading it." Sen. Rep. No. 104-357, at 7 (1996). The government argues that just as "obtaining information" may include merely reading, so too may access be as simple as reading the materials in question.[5] The second Senate Report,

---

[5] The full context for the quote is:

"Information" as used in this subsection includes information stored in intangible form. Moreover, the term "obtaining information" includes merely reading it. There is no requirement that the information be copied or transported. This is critically important because, in an electronic environment, information can be "stolen" without asportation, and the original usually remains intact. This interpretation of "obtaining information" is consistent with congressional intent expressed as follows in connection with 1986 amendments to the Computer Fraud and Abuse statute:

Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the

associated with the 1986 version of the CFAA, notes the intention to criminalize "knowingly trafficking in other people's computer passwords." Sen. Rep. No. 99-432, at 3 (1986), 1986 U.S.C.C.A.N. 2479, 2480. This comment, however, seems to be in reference to § 1030(a)(6) of the CFAA, which criminalizes trafficking in passwords, and is not at issue in the current case. *See id.* at 13.

The Court need not opine on whether § 1030(a) (4) should be read so broadly as to encompass the situation where an unauthorized person looks over the shoulder of the authorized user to view password protected information or files. The allegation in Count Nine is that J.F. logged on to the computer using her credentials, then handed over the computer terminal to M.J., who ran his own searches through the Korn/Ferry database and then downloaded files therefrom.

Functionally and logically, this is no different than if J.F. gave M.J. the password, and M.J. typed in the password himself. The only distinction differentiating the two scenarios is one based on a constrained and hypertechnical definition of "access" in which access focuses solely on the moment of entry and nothing else. Not only would such a definition produce a non-sensical result; it is not supported by the language of the statute. The crime under § 1030(a)(4) is "accessing" a protected computer, or not "entering" or "logging on to" a protected

---

data. Actual asportation, in the sense of physically removing the date from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.

Sen. Rep. No. 104-357, at 7 (1996) (quoting Sen. Report No. 99-432, at 6-7 (1986), 1986 U.S.C.C.A.N. 2479, 2483-2484).

computer. 18 U.S.C. § 1030(a)(4). Nothing in the CFAA suggests anything other than a common definition of the term "access," applies. The Oxford English Dictionary defines "access" as, *inter alia*, "[t]he opportunity, means, or permission to gain entrance to *or use* a system, network, file, etc." *See* Oxford English Dictionary, www.oed.com (emphasis added); *see also* Black's Law Dictionary (defining access as, *inter alia*, "[a]n opportunity or ability to enter, approach, pass to and from, or communicate with"). The common definition of the word "access" encompasses not only the moment of entry, but also the ongoing use of a computer system. Under the facts alleged in the indictment, M.J. "proceeded to query Korn/Ferry's Searcher database and download information, after obtaining initial access." SI ¶ 19*o*. That J.F. entered the password for him rather than having M.J. type it himself does not alter the fact that in common parlance and in the words of the CFAA, M.J. accessed the protected computer system, and he did not have authorization to do so.[6]

---

[6] In his motion, Defendant also argued that the third and eighth counts must be dismissed because the first superseding indictment did not specify who used the Searcher database to download information. The second superseding indictment, however, has remedied this problem by alleging that Christian was the person who accessed the database on both occasions, and that she did so without authorization. SSI ¶ 19. Though the second superseding indictment does not allege who logged into the Korn/Ferry system with respect to count eight, it does allege that it was Christian who ran the queries in the database. For the reasons discussed above with respect to count nine, this is sufficient to allege that Christian accessed the database without authorization, and thus to state a violation of the CFAA.

IV. CONCLUSION

For the foregoing reasons, Defendant's motion to dismiss the third, eighth, and ninth counts of the first superseding indictment is **DENIED**.[7]

This order disposes of Docket Nos. 274 and 276.

IT IS SO ORDERED.

[7] As noted above, the third, eighth, and ninth counts of the first superseding indictment correspond to the third, fourth, and fifth counts of the second superseding indictment.

APPENDIX D

STATUTE INVOLVED

18 U.S.C. § 1030 provides:

Fraud and related activity in connection with computers

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n)[1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

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

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

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

---

[1] See References in Text note below.

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[2]

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;[3]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected

---

[2] So in original. The period probably should be a semicolon.
[3] So in original. Probably should be followed by "or".

computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.