No. 16-1344

In the Supreme Court of the United States

DAVID NOSAL, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

JEFFREY B. WALL
Acting Solicitor General
Counsel of Record
KENNETH A. BLANCO
Acting Assistant Attorney General
JENNY C. ELLICKSON
Attorney

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTIONS PRESENTED

Whether the court of appeals correctly determined that petitioner and his co-conspirators accessed their former employer's computer system "without authorization," within the meaning of 18 U.S.C. 1030, when they used someone else's credentials to access that system after the employer had explicitly revoked their own access rights.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Statutes:

In the Supreme Court of the United States

No. 16-1344

DAVID NOSAL, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINIONS BELOW

The amended opinion of the court of appeals (Pet. App. 1a-70a) is reported at 844 F.3d 1024. The order of the district court denying petitioner's motions for a new trial and for acquittal (Pet. App. 71a-138a) is not published in the *Federal Supplement* but is available at 2013 WL 4504652. The order of the district court denying petitioner's motion to dismiss the indictment (Pet. App. 139a-163a) is reported at 930 F. Supp. 2d 1051. A prior opinion of the court of appeals is reported at 676 F.3d 854.

JURISDICTION

The amended judgment of the court of appeals was entered on December 8, 2016. A petition for rehearing was denied on that date (Pet. App. 2a). On February 24, 2017, Justice Kennedy extended the time within which to file a petition for a writ of certiorari to and including

April 7, 2017. On March 24, 2017, Justice Kennedy further extended the time to and including May 5, 2017, and the petition was filed on that date. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a jury trial in the United States District Court for the Northern District of California, petitioner was convicted on three counts of computer fraud, in violation of 18 U.S.C. 1030(a)(4); one count of unauthorized downloading, copying, and duplicating of trade secrets, in violation of 18 U.S.C. 1832(a)(2) (2000); one count of unauthorized receipt and possession of stolen trade secrets, in violation of 18 U.S.C. 1832(a)(3) (2000); and one count of conspiracy, in violation of 18 U.S.C. 371. C.A. E.R. 169-170, 178-179. He was sentenced to twelve months and one day in prison, three years of supervised release, a $60,000 fine, and a $600 special assessment. *Id.* at 169-175. The court of appeals affirmed. Pet. App. 1a-47a.

1. Petitioner was a high-level regional director at Korn/Ferry International, a global executive-search firm. Pet. App. 6a. In 2004, after being passed over for a promotion, petitioner announced his intention to leave Korn/Ferry. *Ibid.* Petitioner "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." *Ibid.* "As he put it, Korn/Ferry was giving him 'a lot of money' to 'stay out of the market.'" *Ibid.* Nonetheless, petitioner "was very busy, secretly launching his own search firm" with several other Korn/Ferry employees, including Becky Christian, Mark Jacobson, and Jacqueline Froehlich-L'Heureaux. *Id.* at 4a. In 2005, Christian and Jacobson left Korn/Ferry to join the

startup. *Id.* at 7a. At petitioner's request, Froehlich-L'Heureaux remained at Korn/Ferry. *Id.* at 4a.

Petitioner's new venture "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." Pet. App. 7a. The database was "central to Korn/Ferry's work." *Ibid.* Korn/Ferry hosted the database on its internal computer network and considered it confidential. *Id.* at 8a. "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." *Id.* at 19a. Korn/Ferry issued each employee a unique username and password to its computer system, and each new employee signed a confidentiality agreement that prohibited password sharing. *Id.* at 8a.

After petitioner "became a contractor and Christian and Jacobson left Korn/Ferry, Korn/Ferry revoked each of their credentials to access Korn/Ferry's computer system." Pet. App. 8a. Nonetheless, petitioner was not "deterred," and "on three occasions" his co-conspirators Christian and Jacobson acquired access credentials from Froehlich-L'Heureaux and used those credentials to access Korn/Ferry's computer system and retrieve confidential information from Searcher. *Id.* at 8a-9a. Froehlich-L'Heureaux had no authority from Korn/Ferry to provide her password to former employees whose computer access had been revoked, *id.* at 5a, and "she and the others knew that she had no authority to control system access," *id.* at 19a n.7.

Specifically, in April 2005, petitioner "instructed Christian to obtain some source lists from Searcher to expedite their work for a new client." Pet. App. 8a-9a.

"Thinking it would be difficult to explain the request" to Froehlich-L'Heureaux, Christian logged in using Froehlich-L'Heureaux's credentials, ran the queries in Searcher herself, then sent the results to petitioner. *Id.* at 9a. In July 2005, Christian again logged in using Froehlich-L'Heureaux's credentials and ran a custom report and search. Later in July, Jacobson logged in as Froehlich-L'Heureaux, "to download information on 2,400 executives." *Ibid.* "None of these searches related to any open searches that fell under Nosal's independent contractor agreement." *Ibid.*

2. a. A federal grand jury in the Northern District of California returned an indictment charging petitioner with various offenses, including eight counts under the Computer Fraud and Abuse Act of 1986 (CFAA), 18 U.S.C. 1030(a)(4). Pet. App. 9a. Section 1030(a)(4) prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value."

Five of petitioner's eight CFAA counts were based on allegations that Froehlich-L'Heureaux and Christian downloaded material from Searcher using their own credentials while employed at Korn/Ferry, but in violation of company policies. Pet. App. 9a. The district court dismissed those counts, *ibid.*, and the en banc court of appeals affirmed. See 676 F.3d 854, 864 (en banc) (*Nosal I*).

On remand, a federal grand jury issued a second superseding indictment that charged petitioner with three counts of computer fraud, in violation of 18 U.S.C. 1030(a)(4); one count of unauthorized downloading, copying, and duplicating of trade secrets, in violation of

18 U.S.C. 1832(a)(2) (2000); one count of unauthorized receipt and possession of stolen trade secrets, in violation of 18 U.S.C. 1832(a)(3) (2000); and one count of conspiracy, in violation of 18 U.S.C. 371. Pet. App. 10a; C.A. E.R. 1167-1178 (second superseding indictment). The three remaining CFAA counts were based on the three occasions described above, when petitioner's co-conspirators (Christian and Jacobson) accessed Korn/Ferry's computer system by purporting to be Froehlich-L'Heureaux, after Korn/Ferry had revoked their own login credentials. Pet. App. 10a.

b. Petitioner moved to dismiss the three remaining CFAA counts, arguing that the court of appeals' decision in *Nosal I* limited the CFAA to "hacking crimes where the defendant circumvented technological barriers to access a computer." Pet. App. 154a-155a. The district court disagreed with petitioner's interpretation of *Nosal I*, observing that *Nosal I* "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.* at 156a. The court further held that, even if *Nosal I* added a "circumventing technological access barriers" element to crimes under Section 1030(a)(4), the indictment sufficiently alleged such circumvention, because "password protection is one of the most obvious technological access barriers that a business could adopt." *Id.* at 157a (citation omitted). And the court rejected petitioner's contention that "the CFAA does not cover situations where an employee voluntarily provides her password to another," reasoning that petitioner "point[ed] to nothing in the wording of the CFAA or interpretive case law to support [his] construction." *Id.* at 159a

c. At trial, the district court gave the jury the following instruction on the meaning of "without authorization":

> 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.

Pet. App. 24a-25a. "[I]t was not disputed that Korn/ Ferry was the source of permission to grant authorization." *Id.* at 25a. The jury found petitioner guilty on all counts.* *Id.* at 10a.

3. The court of appeals affirmed petitioner's convictions, but vacated the restitution order in part. Pet. 1a-47a.

a. As relevant here, the court of appeals first rejected petitioner's argument that his co-conspirators' use of Froehlich-L'Heureaux's credentials to access Searcher was lawful in light of Froehlich-L'Heureaux's own authority to access Searcher. "Implicit in the definition of authorization," the court stated, "is the notion

* Although petitioner suggests otherwise (Pet. 7), during the proceedings below the government argued that petitioner's convictions on the conspiracy and trade-secrets counts would survive a decision that the conduct in petitioner's case did not violate the CFAA because the evidence of petitioner's trade-secrets crimes was sufficient to sustain those convictions. See Gov't Opp. to Pet. for Reh'g En Banc at 4 n.1.

that someone, including an entity, can grant or revoke that permission." Pet. App. 18a; see also *id.* at 3a-5a. "Here," the court explained, "that entity was Korn/Ferry," and Froehlich-L'Heureaux "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." *Id.* at 18a; see *id.* at 19a (noting that Korn/Ferry "controlled access to its computers" and "retained exclusive discretion to issue or revoke access to the [Searcher] database"). The court explained that once Korn/Ferry revoked petitioner's, Christian's, and Jacobson's login credentials, those former employees were "'outsiders' with no authorization to access Korn/Ferry's computer system." *Id.* at 19a. The court thus concluded that the CFAA "unambiguously" covered petitioner's conduct. *Id.* at 18a n.6 (citation omitted).

The court of appeals added that because petitioner had "received particularized notice of his revoked access," this case presented none of the "difficulties" of "hypotheticals in which a less stark revocation is followed by more sympathetic access through an authorized third party." Pet. App. 19a-20a; see *id.* at 24a. The court reserved those potential "difficulties" for "another day." *Id.* at 20a. The court explained that petitioner's case bore "little resemblance to asking a spouse to log in to an email account to print a boarding pass," but instead presented "the straightforward application of a common, unambiguous term to the facts and context at issue." *Id.* at 24a.

The court of appeals additionally rejected petitioner's argument that the jury instruction was erroneous because it did not inform the jury that a party must circumvent a technological access barrier in order to access a computer "without authorization." Pet. App. 25a. The court explained that the CFAA's statutory language included no such requirement. *Ibid.* The court further concluded that, even if petitioner were correct, any instructional error would be "without consequence" because "[t]he password system adopted by Korn/Ferry is unquestionably a technological barrier designed to keep out those 'without authorization.'" *Id.* at 26a; see *ibid.* ("A password requirement is designed to be a technological access barrier.").

b. Judge Reinhardt dissented. Pet. 48a-70a. In his view, "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." *Id.* at 54a. He thus would have held that the CFAA did not cover use of an employee's password by a former employee whose own access credentials had been revoked. *Id.* at 51a.

ARGUMENT

The court of appeals correctly determined that petitioner and his co-conspirators accessed Korn/Ferry's computer system "without authorization" within the meaning of 18 U.S.C. 1030 when they used someone else's credentials to access that system after their own permission to access it had been specifically rescinded. Petitioner seeks further review on the premise (Pet. i) that the court "held that a computer's owner has exclusive discretion to authorize access" for purposes of the CFAA and that "an account holder cannot independently confer authorization." But the court did not adopt such a blanket rule. Instead, the court explained that "[i]mplicit in the definition of authorization is the notion that *someone*, including an entity, can grant or revoke authorization" and found that, on the facts of this case, "that entity was Korn/Ferry." Pet. App. 18a (emphasis added). That conclusion does not conflict with the decision of any other court of appeals and does not warrant this Court's review.

1. a. Section 1030(a)(4) prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value." 18 U.S.C. 1030(a)(4). Like many federal criminal statutes, the CFAA does not define "authorization" or "without authorization." See 18 U.S.C. 1030(e); Pet. App. 17a & n.5 (collecting other offenses using this phrase, including economic espionage). As the court of appeals below recognized, however, the "ordinary" and "common-sense meaning" of "authorization" is "'permission or power granted by an authority.'" Pet. App. 17a (quoting *LVRC Holdings LLC* v. *Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009), and *Random House Webster's Unabridged Dictionary* 139 (2d ed. 2001)).

The court of appeals correctly applied that definition to affirm the convictions in this case. The trial evidence established that Korn/Ferry "controlled access to its computers, including the Searcher database," and "retained exclusive discretion to issue or revoke access to the database." Pet. App. 19a. Korn/Ferry issued each employee a unique username and password to its computer system, and it required new employees to sign confidentiality agreements that prohibited password sharing. *Id.* at 8a. When petitioner became a contractor and Christian and Jacobson left Korn/Ferry, Korn/Ferry revoked each of their login credentials for the computer system. *Id.* at 8a, 25a. When Froehlich-L'Heureaux later gave Christian and Jacobson her login credentials, "she and the others knew that she had no authority to control system access," *id.* at 19a n.7, and Korn/Ferry had not authorized her to provide her password to former employees whose computer access had been revoked, *id.* at 5a. The court correctly determined that in those circumstances, Christian and Jacobson accessed Searcher "without authorization" when they used Froehlich-L'Heureaux's credentials to gain access to Korn/Ferry's computers, thereby circumventing Korn/Ferry's revocation of their own access credentials. *Id.* at 24a.

b. Contrary to petitioner's contention (Pet. 9), the court of appeals did not hold that, in every case, "a computer's owner has '*exclusive* discretion' to 'issue or revoke access.'" *Ibid.* (quoting Pet. App. 19a). Rather, the court focused on the fact that, in the circumstances of this particular case, Korn/Ferry "retained exclusive discretion to issue or revoke access." Pet. App. 19a. That fact has ample support in the record, particularly when viewed in the light most favorable to the government, and petitioner does not contend otherwise. See, *e.g.*, C.A. E.R. 703-708; C.A. S.E.R. 232-233, 235, 237. The court emphasized that its holding was limited to the facts of petitioner's case, where petitioner "received particularized notice of his revoked access following a prolonged negotiation." Pet. App. 19a-20a. And the court stated that any "difficulties" presented by different, hypothetical cases "in which a less stark revocation is followed by more sympathetic access through an authorized third party" could be "reserved for another day." *Ibid.*

Petitioner is therefore mistaken in claiming (Pet. 2-3, 17-21) that, under the opinion below, the hypothetical fact patterns he describes would be CFAA violations in the Ninth Circuit. Most of petitioner's hypotheticals posit that a computer accountholder in the first instance shared the login credentials for his or her personal online account with a third party, and the third party then used those credentials to access the account with the accountholder's permission but in violation of the relevant website's terms of service. See *ibid.* Nothing in the opinion below suggests that that those fact patterns are CFAA violations in the Ninth Circuit, and the court's decision in *Facebook, Inc.* v. *Power Ventures, Inc.*, 844 F.3d 1058 (2016), petition for cert. pending, No. 16-1105 (filed Mar. 9, 2017)—issued a day after the decision below—confirms that they are not. The court held in *Power Ventures* that "a violation of the terms of use of a website—without more—cannot establish liability under the CFAA." *Id.* at 1067. Applying that principle, the court determined that the defendant in that case did not access Facebook's computers "without authorization," within the meaning of the CFAA, when it accessed specific Facebook accounts with the accountholders' permission. *Ibid.* (stating that the accountholders "took action akin to allowing a friend to use a computer or to log on to an e-mail account"). Instead, a CFAA violation occurred only after Facebook "expressly rescinded [the defendant's] permission" by sending a cease-and-desist letter. *Ibid.*

This case would be a particularly poor vehicle for addressing any question of the CFAA's application to a circumstance in which a person, in the first instance, borrows another person's credentials to access a system. As the court of appeals correctly stated, "[t]his appeal is not about password sharing." Pet. App. 5a. This case also does not involve an authorized user's use of a system in violation of the company "terms of use" policy for how an authorized user should behave when on a system. Indeed, in *Nosal I*, the Ninth Circuit held that the CFAA does *not* criminalize a mere "terms of use" violation. See 676 F.3d at 861 (describing those as "policies that most people are only dimly aware of and virtually no one reads or understands"). Rather, this case involves a fact pattern of clearly unlawful activity in which petitioner, Christian, and Jacobson accessed Searcher surreptitiously by purporting to be Froehlich-L'Heureaux precisely because they lacked authorization to access Searcher themselves after that authorization had been expressly revoked.

2. Petitioner contends (Pet. 9) that the courts of appeals are divided regarding "who may authorize access under the CFAA." Contrary to petitioner's suggestion, no court of appeals has held that, when an employer revokes an employee's credentials to prevent him from continuing to access a system, the employee nonetheless accesses the system "with[] authorization" so long as he surreptitiously borrows a different employee's credentials that have not been revoked. Accordingly, no circuit conflict is implicated here.

a. Petitioner asserts (Pet. 9-11) that the decision below conflicts with *WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F.3d 199 (4th Cir. 2012), cert. denied, 568 U.S. 1079 (2013), and *United States* v. *Valle*, 807 F.3d 508 (2d Cir. 2015). But neither case involved post-revocation surreptitious access, and neither establishes that the convictions in this case would have been reversed in another circuit.

In *WEC*, the Fourth Circuit examined whether an employee accessed his employer's computers "without authorization" when he violated "policies regarding the use of a computer or information on a computer to which [he] otherwise has access." 687 F.3d at 203. In that case, the employer's policies did not restrict the employee's "authorization to access the information," and, in fact, the employer had "authorized his access to the company's intranet and computer servers." *Id.* at 202. The Fourth Circuit concluded, on those facts, that the employee had not accessed the employer's computers "without authorization" under the CFAA because the employer had "approve[d] or sanction[ed] his admission." *Id.* at 204.

In *Valle*, the Second Circuit similarly concluded that a police officer had not violated the CFAA when he accessed law-enforcement databases for personal use, in violation of department policies. 807 F.3d at 511-513. As in *WEC* but unlike here, the officer "had access" to the databases as a result of his employment, subject to the limitation that he access them only in the course of his official duties. *Id.* at 512-513. The question in the case was thus whether the defendant had "exceeded authorized access" under the CFAA; no allegation was made that he had accessed computers "without authorization." See *id.* at 511, 523-524.

WEC and *Valle* are accordingly inapposite. Neither case addressed whether a defendant would access an employer's computer system "without authorization" if the employer had revoked his access to the system, but he nonetheless circumvented that revocation by surreptitiously borrowing another employee's credentials. Rather, both cases involved employees who could access the system themselves, without purporting to be somebody else, and whose access had never been revoked. To the extent that *WEC* and *Valle* might conflict with other circuits' interpretations of the separate statutory phrase "exceeds authorized access" as it relates to a violation of a company's terms of use policy, the court of appeals' decision below does not implicate that conflict. Indeed, the Ninth Circuit's decision in *Nosal I* aligns with the Second and Fourth Circuits' view of "exceeds authorized access." See *Valle*, 807 F.3d at 527 (agreeing with *Nosal I* and *WEC*); *WEC*, 687 F.3d at 203) (agreeing with *Nosal I*). Accordingly, to the extent that petitioner believes that *WEC* and *Valle* correctly construed the phrase "exceeds authorized access," he has already persuaded the court below to adopt that same view.

b. Petitioner additionally errs in contending (Pet. 12-15) that the decision below is in tension with decisions from the First, Fifth, and Seventh Circuits. The rules petitioner purports to derive from those decisions are not contradicted by the decision below and would not change the outcome here.

In *International Airport Centers, L.L.C.* v. *Citrin*, 440 F.3d 418 (2006), the Seventh Circuit addressed whether an employee accessed his employer-issued laptop "without authorization" when, "having already engaged in misconduct and decided to quit * * * in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer." *Id.* at 420 (citation omitted). The court reasoned that the employee's "breach of his duty of loyalty 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.

Petitioner asserts (Pet. 12) that *Citrin*'s analysis "would allow an account holder to delegate access to a third party in appropriate circumstances"—*i.e.*, when "the delegation was consistent with the account holder's duties to the owner." Even assuming that reading of *Citrin* is correct, however, such a rule would not change the outcome here because Froehlich-L'Heureaux violated her duties to Korn/Ferry when she gave her login credentials to Christian and Jacobson, knowing that Korn/Ferry had revoked their credentials to prevent them from accessing its computer system.

In *United States* v. *Phillips*, 477 F.3d 215 (5th Cir.), cert. denied, 552 U.S. 820 (2007), a student at the University of Texas with a university computer account designed a computer program that hacked into a secure university server by guessing the login credentials of authorized users. *Id.* at 217-218. That brute-force attack gave the student a "back door" in the server, and the student thus gained access to data about more than 45,000 people affiliated with the university. *Id.* at 218. In holding that sufficient evidence supported the jury's conclusion that the defendant had accessed the university network "without authorization," the Fifth Circuit explained that "Phillips's brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to computerized data that he was not permitted to view or use." *Id.* at 220.

Petitioner asserts (Pet. 13) that the Fifth Circuit's reasoning in *Phillips* "opens the door to a wide range of access-sharing" and would, for example, allow students to share their school-issued laptops with their parents if the school "would 'reasonab[ly] expect[]' that parents would occasionally use them." *Ibid.* (quoting *Phillips*, 477 F.3d at 220) (brackets in original). Even assuming that reading of *Phillips* is correct, such a rule would not change the outcome here because Korn/Ferry would not have reasonably expected that, after it revoked Christian's and Jacobson's credentials, Froehlich-L'Heureaux would nonetheless give them her own credentials in order to enable them to circumvent the revocation and access Searcher themselves. See, *e.g.*, C.A. E.R. 968 ("If we had seen Searcher as falling within the resources here, we wouldn't have cut off [petitioner's] access."); *ibid*. (following revocation "the use of Searcher was not necessary and actually wasn't provided for in any respect for that reason.").

In *EF Cultural Travel BV* v. *Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), superseded by statute in part on other grounds, see 18 U.S.C. 1030(e)(11), the defendant company used a "scraper" program to retrieve large quantities of proprietary pricing information from the plaintiff company's public website. 274 F.3d at 579-581. Leading that effort was an employee who had previously worked for the plaintiff company and who shared the plaintiff's confidential information with the scraper program's developers, in violation of his confidentiality agreement with the plaintiff. *Id.* at 579, 582-583. Based on those facts, the First Circuit affirmed the district court's issuance of a preliminary injunction in a civil case against the defendant, reasoning in part that the plaintiff would likely prove that the defendant had exceeded authorized access to the plaintiff's website. *Id.* at 581-584. In so doing, that court of appeals expressly declined to resolve the parties' disagreement over the meaning of "without authorization" and declined to decide whether the defendant had accessed the website "without authorization." *Id.* at 581-582 & n.10.

EF Cultural Travel does not support petitioner and is far afield from this case. Petitioner interprets *EF Cultural Travel* as establishing (Pet. 14) that, "[a]bsent 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." Even assuming that reading of *EF Cultural Travel* is correct, however, such a rule would not change the outcome here because in giving her login credentials to Christian and Jacobson, Froehlich-L'Heureaux violated a confidentiality agreement with Korn/Ferry and contravened Korn/ Ferry's clear intent to bar Christian and Jacobson from accessing Searcher.

3. Petitioner briefly contends (Pet. 24-25) that the decision below is incorrect because the district court should have instructed the jury that a person accesses a computer without authorization only "when he circumvents technological access barriers." Pet. 7. That argument does not warrant further review. Petitioner identifies no language in the CFAA that supports a "technological access barrier" rule and identifies no court that has adopted it. Furthermore, even if the CFAA were so limited, the judgment below would still be affirmed because any instructional error would be "without consequence." Pet. App. 26a. The "password system adopted by Korn/Ferry is unquestionably a technological barrier designed to keep out those 'without authorization.'" *Ibid.* This case accordingly would be a particularly poor vehicle for addressing petitioner's argument.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

JEFFREY B. WALL
Acting Solicitor General
KENNETH A. BLANCO
Acting Assistant Attorney General
JENNY C. ELLICKSON
Attorney

SEPTEMBER 2017