FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. DAVID NOSAL, *Defendant-Appellant.*	Nos. 14-10037 14-10275 D.C. No. 3:08-cr-00237-EMC-1 OPINION

Appeal from the United States District Court
for the Northern District of California
Edward M. Chen, District Judge, Presiding

Argued and Submitted October 20, 2015
San Francisco, California

Filed July 5, 2016

Before: Sidney R. Thomas, Chief Judge and Stephen Reinhardt and M. Margaret McKeown, Circuit Judges.

Opinion by Judge McKeown;
Dissent by Judge Reinhardt

SUMMARY*

Criminal Law

The panel affirmed convictions for knowingly and with intent to defraud accessing a protected computer "without authorization," in violation of the Computer Fraud and Abuse Act (CFAA), and for trade secret theft, in violation of the Economic Espionage Act (EEA); and vacated in part and remanded the restitution order for reconsideration of the reasonableness of the attorneys' fees award.

The panel held that the defendant, a former employee whose computer access credentials were revoked, 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 computer data owned by the former employer and to circumvent the revocation of access. The panel rejected the defendant's contentions regarding jury instructions and sufficiency of the evidence in connection with the CFAA counts, as well as his sufficiency-of-the-evidence, instructional, and evidentiary challenges to his EEA convictions for trade secret theft.

The panel determined that the restitution order was within the bounds of the statutory framework set forth in the Mandatory Victim Restitution Act, rejecting the defendant's contention that the award is invalid because it exceeds the actual loss that the district court determined for purposes of the Sentencing Guidelines. Reviewing for abuse of discretion

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

the district court's decision to award nearly $1 million, the panel remanded for the district court to reconsider the reasonableness of the award with respect to the defendant's former employer's attorneys' fees.

Dissenting, Judge Reinhardt wrote that this case is about password sharing, and that in his view, the CFAA does not make the millions of people who engage in this ubiquitous, useful, and generally harmless conduct into unwitting federal criminals.

COUNSEL

Dennis P. Riordan (argued) and Donald M. Horgan, Riordan & Horgan, San Francisco, California; Ted Sampsell-Jones, William Mitchell College of Law, St. Paul, Minnesota; for Defendant-Appellant.

Jenny C. Ellickson (argued), Trial Attorney, Criminal Division, Appellate Section; Leslie R. Caldwell, Assistant Attorney General; Sung-Hee Suh, Deputy Assistant Attorney General; United States Department of Justice, Washington, D.C.; Barbara J. Valliere, Assistant United States Attorney, Chief, Appellate Division; Kyle F. Waldinger and Matthew A. Parrella, Assistant United States Attorneys; United States Attorney's Office, San Francisco, California; for Plaintiff-Appellee.

Jamie Williams, San Francisco, California, for Amicus Curiae Electronic Frontier Foundation.

Martin Hansen, Covington & Burling, Washington, D.C.; Simon J. Frankel and Matthew D. Kellogg, Convington & Burling, San Francisco, California, for Amicus Curiae BSA | The Software Alliance.

David Nied, Keenan W. Ng and Michael S. Dorsi, Ad Astra Law Group, San Francisco, California, for Amicus Curiae NovelPoster.

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. 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.

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 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

[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).

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 access "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 Nosal I*, 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 *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).

[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).

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:

> 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 . . . .

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

[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)).

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 (internal citations omitted) (alteration in original). In 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

[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.

is authorized but who access unauthorized information or files)." *Id.* at 858 (emphasis 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 co-conspirators 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 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).[6]

---

[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").

[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 quotations 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.*

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 give permission to former employees whose access had been categorically revoked by the company.[7] There is no question that Korn/Ferry owned and controlled access to its computers, including the Searcher database, and that it retained exclusive discretion to issue or revoke access to the database. After Nosal's login credentials were revoked on December 8, 2004, he became an "outsider" and was no longer authorized to access Korn/Ferry computers, including Searcher.[8] Christian and Jacobson's credentials were also revoked after they left, at which point none of the three former employees were "insiders" accessing

---

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 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 only entitled 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."

company information. Rather, they were "outsiders" with no authorization to access Korn/Ferry's computer system.[9]

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

---

[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."

[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

"without 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

---

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 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).

> "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 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 willy nilly give 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.

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 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"—but instead relate to a common, unambiguous term. The reality is that facts and context matter in applying the term "without authorization."

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 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 computer data owned by the former employer and to circumvent the 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 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.

[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.

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 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))).

[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.

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*, No. 15-1303, 2016 WL 1458938, at *10 (1st Cir. Apr. 13, 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 . . . .

[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.

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

[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").

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

[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.

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 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 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

[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.

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.

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

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 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, smart-phones, 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.

[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 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.").

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 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

[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.

[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/2013/06/2013-Report.pdf.

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 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]

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.*,

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

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 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

[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)).

believe that he was acting not 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 clear (and public) words of

[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.

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 States v. Kozminski*, 487 U.S. 931, 952 (1988). The majority's construction of the CFAA threatens exactly that. It

[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*.

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 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

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 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

"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.

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 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

[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.

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 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

[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.

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 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.

---

[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.

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.