PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WEC CAROLINA ENERGY SOLUTIONS LLC,

Plaintiff-Appellant,

v.

WILLIE MILLER, a/k/a Mike; EMILY KELLEY; ARC ENERGY SERVICES INCORPORATED,

Defendants-Appellees.

No. 11-1201

Appeal from the United States District Court
for the District of South Carolina, at Rock Hill.
Cameron McGowan Currie, District Judge.
(0:10-cv-02775-CMC)

Argued: April 2, 2012

Decided: July 26, 2012

Before SHEDD and FLOYD, Circuit Judges, and
HAMILTON, Senior Circuit Judge.

Affirmed by published opinion. Judge Floyd wrote the opinion, in which Judge Shedd and Senior Judge Hamilton joined.

COUNSEL

ARGUED: Kirsten Elena Small, NEXSEN PRUET, LLC, Greenville, South Carolina, for Appellant. James William Bradford, Jr., JIM BRADFORD LAW FIRM, LLC, York, South Carolina; Brian S. McCoy, MCCOY LAW FIRM, LLC, Rock Hill, South Carolina, for Appellees. **ON BRIEF:** Mark Gordon, Anthony J. Basinski, PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP, Pittsburgh, Pennsylvania; Angus H. Macaulay, NEXSEN PRUET, LLC, Greenville, South Carolina, for Appellant. Daniel H. Harshaw, BRICE LAW FIRM, LLC, York, South Carolina, for Appellees.

OPINION

FLOYD, Circuit Judge:

In April 2010, Mike Miller resigned from his position as Project Director for WEC Carolina Energy Solutions, Inc. (WEC). Twenty days later, he made a presentation to a potential WEC customer on behalf of WEC's competitor, Arc Energy Services, Inc. (Arc). The customer ultimately chose to do business with Arc. WEC contends that before resigning, Miller, acting at Arc's direction, downloaded WEC's proprietary information and used it in making the presentation. Thus, it sued Miller, his assistant Emily Kelley, and Arc for, among other things, violating the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

The district court dismissed WEC's CFAA claim, holding that the CFAA provides no relief for Appellees' alleged conduct. We agree and therefore affirm.

I.

A.

In 1984, Congress initiated a campaign against computer crime by passing the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. Pub. L. No. 98-473, 98 Stat. 2190. Shortly thereafter, in 1986, it expanded the Act with a revised version, the Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213. Today, the CFAA remains primarily a criminal statute designed to combat hacking. *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009). Nevertheless, it permits a private party "who suffers damage or loss by reason of a violation of [the statute]" to bring a civil action "to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). Notably, although proof of at least one of five additional factors is necessary to maintain a civil action,[1] a violation of any of the statute's provisions exposes the offender to both civil and criminal liability.

Among other things, the CFAA renders liable a person who (1) "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," in violation of § 1030(a)(2)(C); (2) "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," in violation of § 1030(a)(4); or (3) "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[,] or . . . causes damage and loss," in violation of § 1030(a)(5)(B)-(C). Here, WEC

[1]Maintenance of a civil action requires one of the factors outlined in § 1030(c)(4)(A)(i)(I)-(V). Here, WEC alleges that its aggregate losses as a result of Appellees' conduct were "at least $5,000 in value" during a one-year period, which satisfies § 1030(c)(4)(A)(i)(I).

alleges that Miller, Kelley, and Arc violated all three of these provisions.

B.

WEC and Arc are competitors, providing specialized welding and related services to the power generation industry. Both companies are incorporated in South Carolina and maintain their principal places of business in York County, South Carolina. Prior to April 30, 2010, WEC employed Mike Miller as a Project Director and Emily Kelley as his assistant. Both individuals now work for Arc.

When Miller worked for WEC, the company provided him with a laptop computer and cell phone, and authorized his access to the company's intranet and computer servers. According to WEC's complaint, "Miller had access to numerous confidential and trade secret documents stored on . . . computer servers, including pricing terms, pending projects[,] and the technical capabilities of WEC." To protect its confidential information and trade secrets, WEC instituted policies that prohibited using the information without authorization or downloading it to a personal computer. These policies did not restrict Miller's authorization to access the information, however.

On April 30, 2010, Miller resigned from WEC. WEC alleges that prior to resigning, Miller, at Arc's direction, "either by himself or by his assistant, Kelley, downloaded a substantial number of WEC's confidential documents" and emailed them to his personal e-mail address. WEC also alleges that Miller and Kelley downloaded confidential information to a personal computer. Twenty days after leaving WEC, Miller reportedly used the downloaded information to make a presentation on behalf of Arc to a potential WEC customer.

The customer ultimately awarded two projects to Arc. WEC contends that as a result of Miller's and Kelley's

actions, it "has suffered and will continue to suffer impairment to the integrity of its data, programs, systems or information, including economic damages, and loss aggregating substantially more than $5,000 during a one-year period."

In October 2010, WEC sued Miller, Kelley, and Arc, alleging nine state-law causes of action and a violation of the CFAA. Regarding its CFAA claim, WEC averred that Miller and Kelley violated the Act because "[u]nder WEC's policies they were not permitted to download confidential and proprietary information to a personal computer." Thus, by doing so, they "breache[d] their fiduciary duties to WEC" and via that breach, they either (1) lost all authorization to access the confidential information or (2) exceeded their authorization. WEC sought to hold Arc liable because it claimed that Miller and Kelley undertook this conduct as Arc's agents.

Appellees moved for dismissal pursuant to Federal Rule of Civil Procedure 12(b)(6), and the district court held that WEC failed to state a claim for which the CFAA provided relief:

> [I]n this case, WEC's company policies regulated *use* of information not access to that information. Thus, even if Miller and Kelley's purpose in accessing the information was contrary to company policies regulating use, it would not establish a violation of company policies relevant to access and, consequently, would not support liability under the CFAA.

WEC Carolina Energy Solutions, LLC v. Miller, No. 0:10-cv-2775-CMC, 2011 WL 379458, at *5 (D.S.C. Feb. 3, 2011). Thus, it dismissed the CFAA claim and declined to exercise jurisdiction over the remaining state-law claims.[2]

[2]WEC has since moved forward with these claims in South Carolina state court.

II.

We review de novo a district court's dismissal pursuant to Rule 12(b)(6), *Gilbert v. Residential Funding LLC*, 678 F.3d 271, 274 (4th Cir. 2012), accepting as true all factual allegations contained in the complaint, *Erickson v. Pardus*, 551 U.S. 89, 94 (2007)(per curiam).

A.

WEC alleges that Appellees violated §§ 1030(a)(2)(C), (a)(4), (a)(5)(B), and (a)(5)(C), each of which require that a party either access a computer "without authorization" or "exceed[ ] authorized access." The district court held that Appellees' alleged conduct—the violation of policies regarding the use and downloading of confidential information—did not contravene any of these provisions. Accordingly, the crux of the issue presented here is the scope of "without authorization" and "exceeds authorized access." We particularly examine whether these terms extend to violations of policies regarding the use of a computer or information on a computer to which a defendant otherwise has access. Before delving into statutory analysis, however, we briefly review the perspectives of our sister circuits.

In short, two schools of thought exist. The first, promulgated by the Seventh Circuit and advanced by WEC here, holds that when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it. *See Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). Thus, for example, the Seventh Circuit held that an employee who erased crucial data on his company laptop prior to turning it in at the end of his employment violated the CFAA. *Id.* at 419-21. It reasoned that his "breach of his duty of loyalty terminated his agency relationship . . . and with it his author-

ity to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420-21.

The second, articulated by the Ninth Circuit and followed by the district court here, interprets "without authorization" and "exceeds authorized access" literally and narrowly, limiting the terms' application to situations where an individual accesses a computer or information on a computer without permission. *See United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134-35 (9th Cir. 2009). Thus, in *Nosal*, the Ninth Circuit, sitting en banc, held that the defendant's co-conspirators, a group of employees at an executive search firm, did not violate the CFAA when they retrieved confidential information via their company user accounts and transferred it to the defendant, a competitor and former employee. *Nosal*, 676 F.3d at 856, 864. It reasoned that the CFAA fails to provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded. *Id.* at 863-64. As we explain below, we agree with this latter view.

B.

As with any issue of statutory interpretation, we focus on the plain language of the statute, seeking "first and foremost . . . to implement congressional intent." *United States v. Abdelshafi*, 592 F.3d 602, 607 (4th Cir. 2010) (quoting *United States v. Passaro*, 577 F.3d 207, 213 (4th Cir. 2009)) (internal quotation marks omitted). Thus, "'we give the terms [of the statute] their ordinary, contemporary, common meaning, absent an indication [that] Congress intended' the statute's language 'to bear some different import.'" *Id.* (quoting *Stephens ex rel. R.E. v. Astrue*, 565 F.3d 131, 137 (4th Cir. 2009)).

Where, as here, our analysis involves a statute whose provisions have both civil and criminal application, our task merits

special attention because our interpretation applies uniformly in both contexts. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). Thus, we follow "the canon of strict construction of criminal statutes, or rule of lenity." *United States v. Lanier*, 520 U.S. 259, 266 (1997). In other words, in the interest of providing fair warning "of what the law intends to do if a certain line is passed," *Babbitt v. Sweet Home Chapter of Communities for a Great Or.*, 515 U.S. 687, 704 n.18 (1995) (quoting *United States v. Bass*, 404 U.S. 336, 348 (1971)) (internal quotation marks omitted), we will construe this criminal statute strictly and avoid interpretations not "clearly warranted by the text," *Crandon v. United States*, 494 U.S. 152, 160 (1990).

1.

The CFAA is concerned with the unauthorized access of protected computers. Thus, we note at the outset that "access" means "[t]o obtain, acquire," or "[t]o gain admission to." *Oxford English Dictionary* (3d ed. 2011; online version 2012). Moreover, per the CFAA, a "computer" is a high-speed processing device "and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." § 1030(e)(1). A computer becomes a "protected computer" when it "is used in or affecting interstate or foreign commerce." § 1030(e)(2).[3]

With respect to the phrase, "without authorization," the CFAA does not define "authorization." Nevertheless, the Oxford English Dictionary defines "authorization" as "formal warrant, or sanction." *Oxford English Dictionary* (2d ed. 1989; online version 2012). Regarding the phrase "exceeds authorized access," the CFAA defines it as follows: "to access a computer with authorization and to use such access to obtain

[3]Neither party disputes that the computers involved in this case are "protected computers."

or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6).

Recognizing that the distinction between these terms is arguably minute, *see Citrin*, 440 F.3d at 420, we nevertheless conclude based on the "ordinary, contemporary, common meaning," *see Perrin v. United States*, 444 U.S. 37, 42 (1979), 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. *See Brekka*, 581 F.3d at 1133. 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. *See id.* Notably, neither of these definitions extends to the improper *use* of information validly accessed.

2.

WEC presses instead an ostensibly plain-language interpretation articulated in the *Nosal* panel decision, which was subsequently reversed en banc. *See United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012). In that decision, the panel fixated on the word "so" in the definition of "exceeds authorized access." *See id.* at 785. The panel declared that, in context, this conjunction means "in a manner or way that is indicated or suggested." *Id.* (quoting *Webster's Third New Int'l Dictionary* 2159 (Philip Babcock Gove ed., 2002)) (internal quotation marks omitted). Thus, it found that an employee "exceed[s] [his] authorized access" if he uses such access "to obtain or alter information [on] the computer that [he] is not entitled [in that manner] to obtain or alter." *Id.* at 785-86. (third alteration in original) (quoting § 1030(e)(6)) (internal quotation marks omitted). Armed with this interpretation, the court held that the defendant's co-conspirators "exceed[ed] their authorized access" because although they had permission to access the propri-

etary information that they transferred to the defendant, they violated the company's policy regarding the use and disclosure of that information. *See id.* at 787-89. The court reasoned that the co-conspirators' violation of the use and disclosure policy constituted access "in a manner" to which they were not entitled. Thus, they violated the CFAA. *See id.*

As an initial manner, we believe the *Nosal* panel's conclusion is a non sequitur. To us, defining "so" as "in that manner" only elucidates our earlier conclusion that "exceeds authorized access" refers to obtaining or altering information beyond the limits of the employee's authorized access. It does not address the *use* of information after access. Indeed, the Ninth Circuit indicated as much in its en banc reversal, when it declined to hold that the interpretation of "so" as "in that manner" necessarily means employees can be liable for use-policy violations. *See* 676 F.3d at 857. Instead, the court offered hypotheticals illustrating how the panel's interpretation of "so" referred to the means of obtaining information, not the use of information. *See id.* For example, if an employee who has access to view information, but not to download it, disregards company policy by "cop[ying] the information to a thumb drive and walk[ing] out of the building with it," he obtains information "in a manner" that lacks authorization. *Id.* at 858. Similarly, if an employee has complete access to information with his own username and password, but accesses information using another employee's username and password, he also obtains information "in a manner" that is not authorized. *Id.* In contrast, however, where such an employee uses his own username and password to access the information and then puts it to an impermissible use, his "manner" of access remains valid. Thus, in the Ninth Circuit's view, and ours, interpreting "so" as "in that manner" fails to mandate CFAA liability for the improper *use* of information that is accessed with authorization.

Nevertheless, because WEC alleges that Miller and Kelley obtained information by downloading it to a personal com-

puter in violation of company policy, we go a step further. Although we believe that interpreting "so" as "in that manner" fails to subject an employee to liability for violating a use policy, we nonetheless decline to adopt the *Nosal* panel's interpretation of the conjunction. The interpretation is certainly plausible, but it is not "clearly warranted by the text." *Crandon*, 494 U.S. at 160. Indeed, Congress may have intended "so" to mean "in that manner," but it "could just as well have included 'so' as a connector or for emphasis." *Nosal*, 676 F.3d at 858. Thus, faced with the option of two interpretations, we yield to the rule of lenity and choose the more obliging route. "[W]hen [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." *United States v. Universal C. I. T. Credit Corp.*, 344 U.S. 218, 221-22 (1952); *see also Nosal*, 676 F.3d at 863. Here, Congress has not clearly criminalized obtaining or altering information "in a manner" that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter.

And lest we appear to be needlessly splitting hairs, we maintain that the *Nosal* panel's interpretation would indeed be a harsher approach. For example, such an interpretation would impute liability to an employee who with commendable intentions disregards his employer's policy against downloading information to a personal computer so that he can work at home and make headway in meeting his employer's goals. Such an employee has authorization to obtain and alter the information that he downloaded. Moreover, he has no intent to defraud his employer. But under the *Nosal* panel's approach, because he obtained information "in a manner" that was not authorized (i.e., by downloading it to a personal computer), he nevertheless would be liable under the CFAA. *See* § 1030(a)(2)(C). Believing that Congress did not clearly intend to criminalize such behavior, we decline to interpret "so" as "in that manner."

In so doing, we adopt a narrow reading of the terms "without authorization" and "exceeds authorized access" and hold that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access.

3.

In adopting these definitions, we reject any interpretation that grounds CFAA liability on a cessation-of-agency theory. The deficiency of a rule that revokes authorization when an employee uses his access for a purpose contrary to the employer's interests is apparent: Such a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems. We recognize that the Seventh Circuit applied its reasoning to egregious behavior that clearly violated the duty of loyalty. *See Citrin*, 440 F.3d at 419. Nevertheless, we believe that the theory has far-reaching effects unintended by Congress. *See Nosal*, 676 F.3d at 862 (noting that the Seventh Circuit "looked only at the culpable behavior of the defendant[ ] before [it], and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized access'"); *cf.* Restatement (Third) of Agency § 8.01 (2012) ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship."). Although an employer might choose to rescind an employee's authorization for violating a use policy, we do not think Congress intended an immediate end to the agency relationship and, moreover, the imposition of criminal penalties for such a frolic.

III.

WEC founds its CFAA claim on Miller's and Kelley's violations of its policies "prohibiting the use of any confidential

information and trade secrets unless authorized" and prohibiting the "download[ing] [of] confidential and proprietary information to a personal computer." Notably, however, WEC fails to allege that Miller and Kelley accessed a computer or information on a computer without authorization. Indeed, WEC's complaint belies such a conclusion because it states that Miller "had access to WEC's intranet and computer servers" and "to numerous confidential and trade secret documents stored on these computer servers, including pricing, terms, pending projects[,] and the technical capabilities of WEC." Thus, we agree with the district court that although Miller and Kelley may have misappropriated information, they did not access a computer without authorization or exceed their authorized access. *See* 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), (a)(5)(B)-(C). Moreover, because Miller's and Kelley's conduct failed to violate the CFAA, Arc cannot be liable under the statute for any role that it played in encouraging such conduct. Accordingly, we hold that WEC failed to state a claim for which the CFAA can grant relief, *see* Fed. R. Civ. P. 12(b)(6), and we affirm the district court's dismissal of the claim.

IV.

Our conclusion here likely will disappoint employers hoping for a means to rein in rogue employees. But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy. *See Nosal*, 676 F.3d at 863. ("We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals."). Providing such recourse not only is unnecessary, given that other legal remedies exist for these grievances,[4] but

[4]As evidenced by WEC's complaint, nine other state-law causes of action potentially provide relief, including conversion, tortious interference with contractual relations, civil conspiracy, and misappropriation of trade secrets.

also is violative of the Supreme Court's counsel to construe criminal statutes strictly. *Lanier*, 520 U.S. at 266. Thus, we reject an interpretation of the CFAA that imposes liability on employees who violate a use policy, choosing instead to limit such liability to individuals who access computers without authorization or who obtain or alter information beyond the bounds of their authorized access.

AFFIRMED