12 518

No. 12-

IN THE

Supreme Court of the United States

WEC CAROLINA ENERGY SOLUTIONS LLC,

Petitioner,

v.

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

Respondents.

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

PETITION FOR A WRIT OF CERTIORARI

KIRSTEN E. SMALL
Counsel of Record
ANGUS MACAULAY
NEXSEN PRUET, LLC
55 East Camperdown Way (29601)
Post Office Drawer 10648
Greenville, SC 29603-0648
(864) 370-2211
ksmall@nexsenpruet.com

Attorneys for Petitioner
WEC Carolina Energy Solutions, LLC

October 24, 2012
Greenville, South Carolina

244387

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

QUESTION PRESENTED

Congress enacted the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, to provide civil and criminal remedies against individuals who steal information from, or otherwise damage, computers used in interstate commerce. By its terms, the Act applies to both outsiders (*e.g.*, those who hack into a computer network) and insiders (*e.g.*, those who are granted access by their employers). The question presented is one on which the federal courts are deeply divided: Does the CFAA apply to employees who violate employer-imposed restrictions on the purposes for which computer-stored information may be accessed?

CORPORATE DISCLOSURE STATEMENT

Petitioner is 100% owned by its parent company, WEC Welding & Machining, LLC.

TABLE OF CONTENTS

TABLE OF APPENDICES

TABLE OF CITED AUTHORITIES

OPINIONS BELOW

The opinion of the Fourth Circuit Court of Appeals is reported at 687 F.3d 189 (4th Cir. 2012). It is reproduced in the Appendix at 1a-16a. The opinion of the United States District Court for the District of South Carolina is unreported. It is reproduced in the Appendix at 17a-35a.

JURISDICTIONAL STATEMENT

The Fourth Circuit entered its judgment on July 26, 2012. This Court's jurisdiction is premised on 28 U.S.C. § 1254(1).

STATUTORY PROVISION INVOLVED

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, provides in relevant part:

> (a) Whoever—
>
> ...
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> ...
>
> (C) information from any protected computer;
>
> ...
>
> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and

> by means of such conduct furthers the intended fraud and obtains anything of value ...

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

...

(e) As used in this section—

...

> (6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

...

> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. ...

STATEMENT OF THE CASE

A. Introduction

Originally enacted in 1984, the CFAA is designed to punish and deter the theft of information from government computers and computers used in interstate commerce. The CFAA is not merely an "anti-hacking" statute, applicable only to those who infiltrate protected computers from outside the system. Rather, it is undisputed that the CFAA also applies to insiders, *e.g.*, employees who are

granted access to a computer system and the information stored therein. This distinction between outsiders and insiders is expressed in the statutory language of the CFAA, which refers to persons "without authorization"—*i.e.*, outsiders—and to persons who "exceed authorized access"—*i.e.*, insiders. *See also* 18 U.S.C. § 1030(e)(6) (defining "exceeds authorized access").

Under the rule adopted by the Fourth Circuit, an employer can grant or deny access to computer-stored information but cannot set any other limit on access. This distinction is not justified by the statutory text or by common sense, and is contrary to the holdings of at least four other federal appellate courts.

B. Proceedings Below

Petitioner WEC Carolina Energy Solutions, LLC ("WEC") provides specialized welding and related services to the power-generation industry. At the outset of the events relevant to this litigation, Respondent Willie "Mike" Miller was employed by WEC as a Project Manager in Field Services, and Respondent Emily Kelley was his assistant. WEC issued Miller a laptop computer for use in his employment. In order to fulfill the duties of his position, Miller was given access to WEC's computers and servers, and to the numerous confidential and trade secret documents stored therein. This confidential and trade secret information included pricing, terms, pending projects, and information regarding WEC's technical capabilities. WEC has a clear policy prohibiting the use of any confidential information and trade secrets unless authorized by WEC. Both Miller and Kelley were familiar with this policy.

Miller abruptly resigned his employment on April 30, 2010, and went to work for Respondent Arc Energy Services, Inc.—one of WEC's competitors. Immediately before his resignation, Miller, either by himself or with Kelley's help, downloaded a substantial number of WEC's confidential documents and e-mailed the documents to his personal e-mail address. The confidential information taken by Miller and Kelley included past and pending proposals by WEC to its customers, pricing information, and quotation worksheets. Miller and Kelley took these actions at Arc's direction and with the intent to benefit Arc. Furthermore, Arc, through its principals, approved of, encouraged, and benefitted from Miller's and Kelley's illicit actions.

Shortly after he resigned from WEC, Miller made a presentation on behalf of Arc to Dominion Energy for projects at two of Dominion Energy's power plants. In preparing his presentation, Miller used information and documents taken from WEC, including a proposal prepared by WEC for the Dominion projects. Arc was subsequently awarded both projects.

On October 27, 2010, WEC filed this action in the District of South Carolina against Respondents Miller, Kelley, and Arc, asserting claims under state law and for violation of the CFAA. The CFAA count rested on two alternate theories of liability. WEC first alleged that Miller and Kelley acted "without authorization" under the CFAA because, by downloading its proprietary information for the purpose of benefiting Arc, they had violated their duty of loyalty to WEC. Alternatively, WEC alleged that Miller and Kelley had "exceeded authorized access" under the CFAA by downloading WEC's proprietary information for purposes not authorized by WEC.

The district court dismissed the CFAA claim for failure to state a claim upon which relief could be granted. *See* Fed. R. Civ. P. 12(b)(6). The court held that WEC could not state a claim against Miller and Kelley "[b]ecause liability under the CFAA is based on access not use." App. 25a. Once WEC granted Miller and Kelley authority to access its confidential information, the district court reasoned, it was impossible for Miller and Kelley to exceed their authority. Having dismissed the claim that provided the basis for federal jurisdiction, the district court declined to exercise supplemental jurisdiction over the state-law claims, *see* 28 U.S.C. § 1367(c), and dismissed them. App. 32a-34a.

WEC timely appealed the dismissal of the CFAA claim. It filed a separate suit in South Carolina state court alleging the state-law claims. That litigation is ongoing and is not part of these proceedings. Following briefing and oral argument, the Fourth Circuit issued a published opinion affirming the district court.

The Fourth Circuit identified the central issue as "the scope of 'without authorization' and 'exceeds authorized access,'" and the central question as "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." App. 7a. The Fourth Circuit held:

> [An employee] accesses a computer "without authorization" when he gains admission to a computer without approval.... [A]n 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. Notably, neither of these definitions extends to the improper *use* of the information validly accessed.

App. 10a.

REASONS FOR GRANTING THE PETITION

I. The Fourth Circuit's decision widens an existing circuit split regarding the application of the CFAA to employees and former employees.

The Fourth Circuit identified "two schools of thought" regarding the scope of "without authorization or exceeds authorized access." App. 7a. In fact, there are at least three. The two schools of thought identified by the Fourth Circuit are the cessation-of-agency theory, exemplified by the Seventh Circuit's decision in *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), and the code-based theory, articulated by the Ninth Circuit in *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). The third school of thought, like the second, defines authorization in terms of employer-imposed restrictions on access to computer-stored information. But unlike the code-based theory, this third school of thought recognizes that an employee exceeds his authority to access information when he does so for unauthorized purposes.

Cessation of agency. This theory begins with the premise, deeply rooted in agency law, that "authority to act as an agent includes only authority to act *for the benefit of the principal.*" Restatement (Second) of Agency § 39

(emphasis added). When an agent ceases to act for the benefit of his principal, the agent's authority terminates immediately and automatically:

> Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.

Restatement (Second) of Agency § 112.[1] The termination of authority is immediate and automatic, as the illustration makes clear:

> 1. P. employs A, a traveling salesman, to sell goods and receive the price. At the beginning of his trip A embezzles a portion of the amounts received and intends to continue to do so. A is not authorized to continue to sell.

Id. § 112 cmt. b, illus. 1.

Applying these principles, the Seventh Circuit in *Citrin* held that an employee's authorization to access his employer's computer terminates when the employee

1. Justice Scalia discussed the loss of an agent's authority under § 112 in *Holland v. Florida*, 130 S. Ct. 2549 (2010). In *Holland*, the Supreme Court held that a death row inmate was entitled to equitable tolling of the limitations period for a federal habeas corpus petition because his attorney had failed to respond to his repeated inquiries regarding the status of the case. Justice Scalia dissented, arguing that the circumstances did not justify a departure from the usual rule that "[b]ecause the attorney is the litigant's agent, the attorney's acts "or failures to act) within the

uses the computer contrary to the employer's interests, thereby breaching his duty of loyalty to his employer. *See Citrin*, 440 F.3d at 420-21. The employee in *Citrin* had decided to start his own competing business and erased all data from his work computer which included confidential information of his employer that showed that he had engaged in misconduct while employed. The court held that when the employee breached his duty of loyalty to his employer, his agency relationship terminated "and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* Because of that breach of loyalty, the Seventh Circuit held that the employee's actions in deleting or erasing the information were "without authorization."

Code-based access restrictions. Under this interpretation of the CFAA, "a person who 'exceeds authorized access' ... has permission to access the computer, but accesses information on the computer that the person is not entitled to access." In other words, an employer can only grant or deny access to computer-stored information; it cannot set enforceable terms governing access.

Purpose-based access restrictions. The third school of thought, which has been adopted by the First, Third, Fifth, and Eleventh Circuits, recognizes that an employee's authority to access information is properly defined in terms of the purposes for which access is allowed. In other

scope of representation are treated as those of the client." *Id.* at 2571 (Scalia, J., dissenting). Citing § 112, Justice Scalia explicitly distinguished the situation of an attorney's "conduct amounting to disloyalty or renunciation of his role, which *would* terminate his authority." *Id.* at 2573 n.9 (emphasis original).

words, authority to access information for one purpose does not confer authority to access that information for another purpose. Thus, an employee "exceeds authorized access" by violating employer-imposed restrictions on the purpose for which computer-stored information may be obtained. *See, e.g.*, *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that employee exceeded authorized access when he violated employer policy by obtaining information for non-business purpose); *United States v. John*, 597 F.3d 283, 272 (5th Cir. 2010) (holding that because "an employment agreement can establish the parameters of 'authorized' access," "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized'"); *P.C. Yonkers, Inc. v. Celebrations The Party & Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005) (recognizing that the CFAA's reach extends to actions against "former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001) (holding that former employees exceeded authorized access by violating a confidentiality agreement that prohibited the use of information "contrary to the best interests" of the plaintiff).

These various interpretations of the CFAA are irreconcilable. This Court should grant certiorari to resolve the conflict and to provide guidance to the lower courts.

II. The Fourth Circuit's holding, that the CFAA does not apply to purpose-based restrictions on access, is incorrect.

The Fourth Circuit joined the Ninth Circuit in interpreting "exceeds authorized access" as applying only when an employee accesses computer-stored information that he is not permitted to access. The court's reasoning, as explained below, is deeply flawed. Moreover, the Fourth Circuit made no attempt to explain its rejection of the holdings of the four circuits that have recognized the enforceability of purpose-based access restrictions.

The essential flaw of the Fourth Circuit's reasoning is its failure to recognize that the purpose for which an employer authorizes access to information is an inseparable component of the authorization itself. Moreover, a purpose-based restriction on access to information is distinct from a restriction on the use of such information. The Fourth Circuit's hypothetical of the employee who violates company policy by "downloading information to a personal computer so that he can work at home," App. 13a, elides this distinction. The employee who is authorized to obtain computer-stored information to create reports remains within the bounds of authorized access so long as he is, in fact, using the information to create his reports. Downloading the information to a personal computer might be a breach of security, but it is not overstepping the employee's authority to access the information in the first instance.

The Fourth Circuit's failure to appreciate this distinction led it to the false assumption that applying the CFAA to purpose-based access restrictions would

render employees civilly and criminally liable for *de minimis* misconduct, such as accessing the Internet during working hours. App. 14a. This "sky is falling" scenario rests on a fundamental misunderstanding of the CFAA. In enacting and amending the CFAA, Congress has been largely unconcerned with mere *use* of computers. Rather, the central concern of the CFAA is the *protection of information* that is stored on a computer or server. For example, a defendant violates subsection (a)(2), only by using computer access to obtain information. Similarly, subsection (a)(4) applies only when the defendant has obtained "anything of value" *other than mere use of the computer*, unless the computer use itself is of substantial monetary value. Indeed, the CFAA defines "exceeds authorized access" in terms of obtaining or altering "information *in the computer*." *Id.* § 1030(e)(6). An employee who surfs the Internet when he should be working may be using the computer in a way that violates his employer's policies, and he may obtain information (such as a sports score). But such an employee is not violating the CFAA, because information available on the Internet is not information "in the computer."

The Fourth Circuit incorrectly described the CFAA as a statute primarily aimed at computer hackers, *i.e.*, those who break into a system from outside. App. 16a. The statutory language, however, makes clear that Congress was just as concerned with theft and damage caused by employees as it was with the activities of outside computer hackers. The CFAA provides for civil and criminal liability for persons who are "without authorization" to access a computer system and also for persons who "exceed [their] authorization." If Congress were concerned only with computer hackers—those who break into a

computer system from outside—the CFAA would apply only to persons acting "without authorization." But the Act plainly sweeps more broadly, covering insiders who are authorized to use a computer system—such as employees—but who exceed the bounds of that access. The CFAA thus plainly contemplates that an employee may be held liable (criminally or civilly) for violating the Act.

It was also error for the Fourth Circuit to use the rule of lenity as a primary rule of construction. App. 8a-9a. The rule of lenity is not a guiding principle of statutory construction; it is a tie-breaker of last resort. As this Court recently explained, "The rule ... is reserved for cases where, after seizing everything from which aid can be derived, the Court is left with an ambiguous statute." *DePierre v. United States*, 131 S. Ct. 2225, 2237 (2011) (internal quotation marks omitted). If "traditional tools of statutory construction ... suffice to resolve the interpretive issues," there is "no occasion for resort to the rule of lenity." *United States v. Gosselin World Wide Moving, N.V.*, 411 F.3d 502, 514 (4th Cir. 2005). Even if there were some ambiguity in the CFAA, its status as a criminal statute does not require this Court to adopt the narrowest possible construction of its terms. "The canon in favor of strict construction (of criminal statutes) is not an inexorable command to override common sense and evident statutory purpose.... Nor does it demand that a statute be given the narrowest meaning." *United States v. Moore*, 423 U.S. 122, 145 (1975) (internal quotation marks omitted).

CONCLUSION

A reality of our increasingly digital world is that a business's most vital information is likely to be stored in a computer server instead of a file cabinet. The Fourth Circuit's decision deprives employers like WEC of the CFAA's protections precisely where those protections are most needed: to deter and punish the theft of highly sensitive or confidential information by employees who must be given access to that information to perform their jobs.

This Court should grant certiorari to resolve the division among the circuit courts of appeals as to the proper interpretation of the CFAA.

Respectfully submitted,

KIRSTEN E. SMALL
Counsel of Record
ANGUS MACAULAY
NEXSEN PRUET, LLC
55 East Camperdown Way
(29601)
Post Office Drawer 10648
Greenville, SC 29603-0648
(864) 370-2211
ksmall@nexsenpruet.com

Attorneys for Petitioner WEC Carolina Energy Solutions, LLC

October 24, 2012
Greenville, South Carolina