No. 20-575

In The
Supreme Court of the United States

ROYAL TRUCK & TRAILER SALES AND SERVICES, INC.,
Petitioner,

v.

MIKE KRAFT AND KELLY MATHEWS A/K/A KELLY SCHLIMMER
Respondents.

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

MIKE KRAFT AND KELLY MATHEWS A/K/A KELLY SCHLIMMER'S BRIEF IN OPPOSITION

Richard T. Hewlett (*Counsel of Record*)
Salvatore J. Vitale
Jordan Giles
39500 High Pointe Blvd, Suite 350
Novi, MI 48375
(248) 567-7426
rthewlett@varnumlaw.com
sjvitale@varnumlaw.com
jcgiles@varnumlaw.com
Counsel for Respondents Mike Kraft and Kelly Mathews A/K/A Kelly Schlimmer

QUESTION PRESENTED

Whether an employee authorized to access information on a company computer can violate Section 1030(a)(2) of the Computer Fraud and Abuse Act by violating her employer's employee guidelines.

PARTIES TO THE PROCEEDING

1. Royal Truck & Trailer Sales and Services, Inc.
2. Mike Kraft – defendant-respondent
3. Kelly Mathews a/k/a Kelly Schlimmer – defendant-respondent.

STATEMENT OF RELATED PROCEEDINGS

There are no proceedings that are directly related to this case.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

OPINIONS BELOW

The Sixth Circuit's Opinion dated September 9, 2020 is reported at 974 F.3d 756. The district court's opinion has not yet been published, but is reported at 2019 WL 1112387.

STATEMENT OF JURISDICTION

Petitioner filed petition for a writ of certiorari on September 26, 2020, after the Sixth Circuit issued its opinion on March 11, 2019. *Royal Truck & Trailer Sales and Service, Inc. v. Mike Kraft and Kelly Mathews a/k/a Kelly Schlimmer*, 974 F.3d 756 (6th Cir. 2020), *petition for cert. filled*, (U.S. Sept. 26, 2020) (No. 20-575). Petitioner invokes the jurisdiction of this Court pursuant to 28 U.S.C. § 1254(1). *Id.* at 1.

FEDERAL STATUTORY PROVISIONS INVOLVED

28 U.S.C. § 1030(a)(2)(C):

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

(C) information from any protected computer;

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

(emphasis added)

28 U.S.C. § 1030(g):

(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 . . . .

28 U.S.C. § 1030(e)(6):

(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 . . .

STATEMENT OF THE CASE

I. The Computer Fraud and Abuse Act

"The CFAA is criminal, anti-hacking statute that also creates a private cause of action for '[a]ny person who suffers damage or loss by reason of a violation of this section[.]'" Pet. App. 20. (citing 18 U.S.C. § 1030(g)). While the CFAA was initially a criminal statute, Congress added a private cause of action for individuals to recover damages arising out of a violation of the statute in 1994. An individual violates the CFAA when he or she "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any protected computer." 18 U.S.C. § 1030. The CFAA defines the phrase "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The interpretation of this definition has evolved as the circuit courts have grappled with the increased presence of computer and computer use policies in daily life. The early circuit court interpretations of "exceeds authorized access" adopted a broad approach. Therefore, in the First, Fifth, Seventh, and Eleventh Circuits, a person violates the CFAA if that person accesses a computer with permission, but uses the information obtained in a manner that "exceeds" the scope of that person's permitted use. See *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440

F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir. 2001).

However, with the "benefit of a national discourse on the CFAA" and recognizing that "defining 'authorized access' according to the terms of use of a software or program risks criminalizing everyday behavior," the circuit courts began to apply a more modern, narrow interpretation. *EarthCam, Inc. v. OxBlue Corp.*, 703 F. App'x 803, 808 (11th Cir. 2017). Under this narrow approach, applied by the Sixth Circuit in this matter as well as the Second, Fourth, and Ninth Circuits before it, a person only violates the CFAA if that person accesses a computer without permission. See Pet. App. 1; *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc).

II. Factual Background

Respondents Mike Kraft ("Kraft") and Kelly Mathews ("Mathews") (collectively "Respondents") are former employees of Petitioner-Plaintiff Royal Truck & Trailer Sales and Service, Inc. ("Petitioner"). Pet. App. 3. Petitioner provided Respondents with its "Employee Handbook" which "prohibited a range of conduct, including: personal activities; unauthorized use, retention, or disclosure of any of Royal's resources or property; and sending or posting trade secrets or proprietary information outside the organization." *Id.* Petitioner also had another policy prohibiting the employees from removing information or disclosing confidential information obtained from such devices. *Id.*

In February of 2018, Respondents resigned from their employment with Petitioner. *Id.* Petitioner alleges that it began investigating Respondents' conduct during their final days of employment after Respondents' resignation. *Id.* The investigation allegedly revealed that Respondents forwarded information to their respective personal email accounts and restored or reinstalled the operating systems on their company devices. *Id.* at 3-4. Following this discovery, Petitioner filed its Complaint with the District Court for the Eastern District of Michigan, asserting that Respondents' conduct violated the CFAA as well as Michigan law.

III. Procedural History

On April 17, 2018, Respondents moved to dismiss Petitioner's CFAA claims pursuant to Rule 12(b)(6). See Pet. App. 16. Respondents also asked the court to decline supplemental jurisdiction over the seven counts addressing state law and common law claims under Rule 12(b)(1) for Want of Subject Matter Jurisdiction. *Id.* On March 11, 2019, the district court dismissed the two CFAA claims and declined to exercise supplemental jurisdiction over the remaining claims. *Id.*

Petitioner appealed. *Id.* On September 9, 2020, the Sixth Circuit affirmed the district court, holding that the "CFAA prohibits accessing data one is not authorized to access" but not improper use of that data. Pet. App. at 9. The court below reasoned that because Respondents had authorization to access Petitioner's information, "their conduct did not 'exceed' their 'authorized access,' as those terms are used in § 1030(a)(2)." *Id.* Petitioner filed its Petition for Writ of Certiorari on September 26, 2020.

REASONS FOR DENYING THE PETITION

I. The development of the modern, narrow approach in interpreting 28 U.S.C. § 1030(a)(2) will continue without the intervention of this Court.

Petitioner's 28 U.S.C. § 1030(a)(2) ("§ 1030(a)(2)") claims rest upon one issue—whether "exceeds authorized access" includes situations where a party's access was authorized but his manner of *use* was not. Eight United States Courts of Appeals have interpreted the meaning of "exceeds authorized access" under § 1030(a)(2).[1] In 2001, an early version of the so-called "broad approach" was first adopted by the First Circuit in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir. 2001) based on the proposition that an employee's authorization to access an employer's information ceased upon his breach of an employee's duty of loyalty. In the years that followed, other circuits began to apply the "broad approach" to find a violation of the CFAA where an employee violated an employer's policies regarding access and use of computers. See *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir. 2001); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

The Ninth Circuit was the first to apply the "narrow" approach in interpreting the CFAA's "exceeds authorized access" provision, holding that "the phrase 'exceeds

[1] Petitioner suggests that nine circuits have addressed the "circuit split" regarding the interpretation of 28 U.S.C. § 1030(a). *Royal Truck & Trailer Sales and Services, Inc. v. Mike Kraft and Kelly Mathews a/k/a Kelly Schlimmer,* 974 F.3d 756 (6th Cir. 2020), *petition for cert. filled*, (U.S. Sept. 26, 2020) (No. 20-575) at 19. However, Petitioner misstates the holding of *United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011). The *Teague* opinion did not interpret 28 U.S.C. § 1030(a). *Id.* at 3. Instead, *Teague* addressed whether, under 28 U.S.C. § 1030, the evidence at issue supported the conviction and whether denial of an expert resulted in an unfair trial. *Teague*, 646 F.3d 1119.

authorized access' in the CFAA does not extend to violations of use restrictions." See *LVRC Holdings L.L.C. v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). Subsequently, the Ninth Circuit further clarified the "narrow approach" and explained that "exceeds authorized access" refers only to "individuals whose initial access to a computer is authorized but who access unauthorized information or files." *U.S. v. Nosal*, 676 F.3d 854 (9th Cir., 2012).

In support of its finding, the Ninth Circuit noted the potentially far-reaching effects of the criminalization of an employer's use restrictions:

> Employer-employee and company-consumer relationships are traditionally governed by tort and contract law; the government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law.

Nosal, 676 F.3d at 863. The Ninth Circuit also relied upon the rule of lenity, requiring the court to avoid broad interpretations if "it would 'criminalize a broad range of day-to-day activity." *Nosal*, 676 F.3d at 862-63 (citing *United States v. Kozminski*, 487 U.S. 931, 949 (1988)).

Those circuits addressing the "exceeds authorized access" question after *Nosal* have adopted the narrow approach outlined therein. Just a few months after the *Nosal* decision, the Fourth Circuit followed suit. See *WEC*, 687 F.3d 199, 203 (citing *Nosal*, 676 F.3d at 863). Three years later, the Second Circuit joined the Fourth and Ninth Circuits in adopting the "narrow" approach. See *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015). While detailing the statutory history of the CFAA, the Second Circuit noted that "[t]he Senate Committee Report to the 1986 amendments

specifically described 'exceeds authorized access' in terms of trespassing into computer systems or files." *Id.* at 525 (citing S. Rep. No. 99-432, at 2483).

Finally, the Sixth Circuit in this matter adopted the "narrow" approach and refused to expand the application of the CFAA to any subsequent misuse of information accessed with authorization. *See* Pet. App. 1. In adopting this approach below, the Sixth Circuit found no need to rely on the rule of lenity or legislative history in interpreting the CFAA's definition of "exceeds authorized access." *Id.* at 10-11. Instead, the court relied upon its prior definition of "authorization" and the common definitions of the words "obtain" and "access":

> Reading these definitional provisions together, it follows that in utilizing the phrase "exceeds authorized access," the CFAA targets one who initially "gain[s] entrance to ... a system, network, or file" with "sanction or permission," and then "gain[s] or attain[s]" "information" that, in the words of the statute, she is "not entitled so to obtain...." 18 U.S.C. § 1030(e)(6). [*Id.* at 8.]

Accordingly, the court below held that the "CFAA prohibits accessing data one is not authorized to access." *Id.* at 9.

As circuits adopted the more modern, "narrow" approach, those circuits that had previously applied the "broad approach" began to recognize the criticisms of the "broad approach" and soften their position. For example, the Fifth Circuit, despite previously applying the "broad approach," later cited *Nosal* in distinguishing between an "insider" who "exceeds authorized access" and an "outsider" who acts without authorization and limiting the application of the "broad approach" to outsiders. *United States v. Thomas*, 877 F.3d 591, 596 (5th Cir. 2017). The Fifth Circuit expressed further support of the "narrow approach," stating:

> Indeed, *Brekka* begins its analysis by recognizing that "authorization" has the ordinary meaning of "permission"; the separate term "exceeds authorized access" is the source for its conclusion that access without authorization must be an all-or-nothing proposition. *Id.* at 1133. In addition to its support in the bifurcated statutory scheme for access crimes***, a narrow reading of those statutes avoids criminalizing common conduct—like violating contractual terms of service for computer use or using a work computer for personal reasons—that lies beyond the antihacking purpose of the access statutes.***

Thomas, 877 F.3d at 596 (emphasis supplied).

Likewise, the Eleventh Circuit has expressed uncertainty as to whether application of the broad approach was even a "valid reading" of its opinion in *Rodriguez,* stating "Although it is not entirely clear, one of the lessons from *Rodriguez* may be that a person exceeds authorized access if he or she uses the access in a way that contravenes any policy or term of use governing the computer in question." *EarthCam, Inc.,* 703 F. App'x at 808. The *EarthCam* Court noted the significant criticism the "broad approach" had endured throughout other courts for its potential to criminalize non-criminal behavior:

> We decided *Rodriguez* in 2010 without the benefit of a national discourse on the CFAA. Since then, several of our sister circuits have roundly criticized decisions like *Rodriguez* because, in their view, simply defining "authorized access" according to the terms of use of a software or program risks criminalizing everyday behavior. See *United States v. Valle*, 807 F.3d 508, 527 (2d Cir. 2015; *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) ; *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012) (en banc). Neither the text, nor the purpose, nor the legislative history of the CFAA, those courts maintain, requires such a draconian outcome. We are, of course, bound by *Rodriguez*, but note its lack of acceptance. [*Id.* at 808 fn 2.]

The negative treatment of the "broad approach" by those circuits that originally adopted it suggests the conflict raised by Petitioner as grounds for

Certiorari will be resolved by subsequent opinions narrowing the scope of the "broad approach" or overruling it entirely *en banc*. Therefore, the Court should deny Certiorari.

II. The Court should deny certiorari as the Court's forthcoming opinion in *Van Buren v. United States* will resolve any conflict between the circuits.

Van Buren, a criminal case addressing whether access for an improper purpose constitutes a violation of the CFAA, was recently argued before this Court. *Van Buren v. United States*, 940 F.3d 1192 (11th Cir. 2019), *oral argument*, 206 L. Ed. 2d 822 (Nov. 30, 2020) (No. 19-783). While the Court has yet to issue its opinion on the matter, the Court's decision in *Van Buren* will resolve the circuit courts' conflicting interpretations of the CFAA. See Petition at 2 (question presented citing *Van Buren*). In fact, the Sixth Circuit acknowledged the likelihood that this Court could resolve the issue of interpreting "exceeds authorized use" via its grant of certiorari in *Van Buren v. United States*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 206 L. Ed. 2d 822 (Apr. 20, 2020) (No. 19-783). Pet. App. 1.

In its request for Certiorari, Petitioner relies upon the potential for "ambiguity that may result from interpreting the statute in the context of solely a criminal case." See Pet. Brief at 27. No such risk of ambiguity exists. As this Court stated in *Leocal v. Ashcroft*, 543 U.S. 1, fn. 8 (2004), "we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context." See also *United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517–518, and n. 10 (1992) (plurality opinion).

The Court's ultimate decision in *Van Buren*, despite its criminal context, will equally apply to civil claims under the CFAA, eliminating any need for the Court to resolve the disagreement between the circuit courts. Thus, the issue presented by Petitioner to this Court will effectively become moot. Therefore, this Court should deny Petitioner's writ.

III. This Court's review is unwarranted because Congress is better suited to address its intention to impose criminal and civil liability regarding hacking.

Congress is more than capable of refining or changing the CFAA to create civil and criminal liability for breaching the duty of loyalty as the "broad' approach would require. "Congress alone has the institutional competence, democratic legitimacy, and (most importantly) constitutional authority to revise statutes in light of new social problems and preferences. Until it exercises that power, the people may rely on the original meaning of the written law." *Wisconsin Cent. Ltd. v. United States*, 138 S. Ct. 2067, 2074 (2018).

As the Sixth Circuit noted in its decision below, "Congress surely knew how to say, 'exceeds authorized use' or otherwise proscribe using data for unauthorized purposes." Pet. App. 9. "Yet it did not do so in the CFAA." *Id.* "Where Congress knows how to say something but chooses not to, its silence is controlling." *Griffith v. United States*, 206 F.3d 1389, 1394 (11th Cir. 2000).

Given the broad scope of behaviors prohibited by many websites' boilerplate "terms of use" and employers' internet policies, a piecemeal judicial interpretation of an outdated statute will inevitably give rise to unintended criminal and civil liability. As the Sixth Circuit noted, the "broad" approach would allow employers to define the

scope of criminal liability as opposed to Congress. Pet. App. 13. Because of the policy implications at issue and Congress' ability to clarify when the CFAA would invoke criminal liability, this Court should allow Congress to speak on the matter first and deny certiorari.

CONCLUSION

The petition for writ of certiorari should be denied.

Respectfully submitted,

VARNUM LLP

By: */s/ Richard T. Hewlett*
Counsel of Record

Richard T. Hewlett (Counsel of Record)
Salvatore Vitale
Jordan Giles
Attorneys for Respondents
39500 High Point Blvd. Suite 350
Novi, MI 48375
(248) 567-7400
rthewlett@varnumlaw.com
sjvitale@varnumlaw.com
jcgiles@varnumlaw.com