United States Court of Appeals for the Second Circuit

August Term 2022
No. 21-3089

UNITED STATES OF AMERICA,
Appellee,

v.

MEDGHYNE CALONGE, AKA SEALED DEFENDANT 1,
Defendant-Appellant.

On Appeal from the United States District Court
for the Southern District of New York

ARGUED: MARCH 24, 2023
DECIDED: JULY 14, 2023

Before: PARKER, LYNCH, LOHIER, *Circuit Judges*.

Defendant-Appellant Medghyne Calonge appeals from a judgment of conviction in the United States District Court for the Southern District of New York (Woods, *J.*). Calonge was convicted on two counts of violating the Computer Fraud and Abuse Act. 18 U.S.C.

§ 1030(a)(5)(A)–(B). On appeal, she argues that the government failed to prove that venue was proper in the Southern District of New York. We hold that the government adduced evidence sufficient to prove that Calonge damaged a protected computer within that District and that venue was therefore proper. **AFFIRMED**.

KENDRA L. HUTCHINSON, Federal Defenders of New York, Inc., Appeals Bureau, New York, NY, *for Defendant-Appellant*.

TIMOTHY V. CAPOZZI, Assistant United States Attorney (Louis A. Pellegrino, Won S. Shin, Assistant United States Attorneys, *Of Counsel*), *for* Damian Williams, United States Attorney for the Southern District of New York, *for Appellee*.

PARKER, *Circuit Judge*:

Defendant-Appellant Medghyne Calonge appeals from a judgment of conviction entered in the United States District Court for the Southern District of New York (Woods, *J.*) following her conviction on two counts of violating the Computer Fraud and Abuse Act ("CFAA"). *See* 18 U.S.C. § 1030(a)(5)(A)–(B).

Calonge's primary contention in this appeal is that the government adduced insufficient evidence to prove that venue was proper in the Southern District of New York. We hold that because the government's evidence was sufficient to prove that a protected computer was damaged in the Southern District of New York, venue

was appropriate. We therefore **AFFIRM** the judgment of conviction.

I. BACKGROUND

In 2019, Calonge was hired as the Florida-based human resources manager of 1-800-Accountant, a virtual accounting firm that provides accounting services to a variety of businesses. A major aspect of 1-800-Accountant's business is the creation and maintenance of a database of accountants who can be hired by its clients. To perform these functions, 1-800-Accountant contracted with a software vendor, JazzHR, to create an applicant tracking system database to manage recruiting and keep track of the various accountants with whom 1-800-Account worked. App'x at 74. As a human resources manager, Calonge had "super administrator" access to the JazzHR applicant tracking system. *Id.* Amy Gaspari was Calonge's supervisor and was based at the company's headquarters on Madison Avenue in Manhattan, New York.

Calonge struggled with her work responsibilities. In June 2019, Gaspari concluded that Calonge had improperly locked another employee out of another human resources software program, preventing him from performing his job, and decided to terminate her. On Friday, June 28, 2019, Gaspari had two Florida-based employees hand-deliver a termination letter to Calonge as Gaspari informed Calonge of her termination over the phone. After Calonge was fired, most of her computer log-in credentials were revoked, but Gaspari neglected to revoke her access to the JazzHR database.

That weekend, an employee informed Gaspari that he was unable to access the JazzHR database. On the following Monday, another employee based, like Gaspari, in New York, informed Gaspari that she also could not access that database. Eventually, Gaspari successfully logged in to the JazzHR database but found that

nearly all the information on it had been deleted, including other employees' accounts, 17,000 job applications, documents, resumes, job postings, and so on. Gaspari contacted JazzHR support staff, who produced a log showing that an account associated with Calonge had deleted the data between Friday evening and Sunday morning. 1-800-Accountant was able to recover a small portion of the lost data, and even after it spent more than $140,000 and "six or eight weeks or more" attempting to reconstruct the database after Calonge's deletions, the rebuilt database was "just a shell" of its former self. App'x at 177–78.

As a result of these deletions, Calonge was prosecuted and charged with two counts of violating subsections 1030(a)(5)(A) and 1030(a)(5)(B) of the CFAA, 18 U.S.C. § 1030. Section 1030(a)(5)(A) criminalizes "knowingly caus[ing] the transmission of a program, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." Section 1030(a)(5)(B), meanwhile, criminalizes "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage."

At trial, Gaspari was asked specifically about the effect of Calonge's weekend spree on Gaspari's ability to access the deleted data "from [Gaspari's] computer in New York," and "from [her] office in New York." App'x at 170–71. She responded that Calonge had deleted the JazzHR accounts of 13 employees at the Manhattan office of 1-800-Accountant and that she was herself unable to access the deleted data from her desktop computer in New York. "We had no access to any of the data that was deleted," she explained at trial. App'x at 170. It was "just gone." *Id.*

In addition, JazzHR's director of technical operations testified that the data that Calonge had deleted resided on servers that were

located in Virginia and California in Amazon Web Services data centers.

After the government rested, Calonge moved under Federal Rule of Criminal Procedure 29 for a judgment of acquittal and renewed the motion at the conclusion of the trial. She argued that the evidence was insufficient to prove that venue was proper in the Southern District of New York because there was no evidence that the data Calonge deleted physically "resided" in the district. If the data did not reside in the Southern District of New York, Calonge argued, she could not have damaged a computer there. The government argued that venue was proper wherever damage to a protected computer occurred and that the inability to access the deleted data from a computer in New York constituted "damage" to that computer. The district court denied Calonge's motion and ruled that venue was proper wherever damage to a protected computer occurred. Accordingly, the district court charged the jury that "if you find that the defendant's actions caused damage to a protected computer, venue is proper wherever that damage occurred." App'x at 577. Calonge was found guilty on both counts and sentenced to time-served and three years of supervised release. This appeal followed.

II. DISCUSSION

The Constitution twice protects defendants' venue rights. First, Article III provides that "the Trial of all Crimes . . . shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. In addition, the Sixth Amendment provides that "the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." *Id*. amend. VI. The purpose of these provisions is to

"protect defendants from the bias and inconvenience that may attend trial in a forum other than one in which the crime was committed." *United States v. Rowe*, 414 F.3d 271, 277 (2d Cir. 2005) (citing *United States v. Johnson*, 323 U.S. 273, 275, 278 (1944); *United States v. Cores*, 356 U.S. 405, 407 (1958)).

Because venue is not an element of a crime, it can be proven by a preponderance of the evidence, rather than beyond a reasonable doubt. *United States v. Davis*, 689 F.3d 179, 185 (2d Cir. 2012). The sufficiency of the evidence to support venue is a question of law that we review *de novo*. *See id.*

In a small subset of cases, determining the location where a crime was committed is not a straightforward exercise. If an offense is committed in multiple places – interstate kidnapping, for example – it may be "prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237; *see United States v. Rodriguez-Moreno*, 526 U.S. 275, 282 (1999).

The proliferation of Internet-related crimes has further complicated the issue of appropriate venue. *See United States v. Auernheimer*. 748 F.3d 525, 541 (3d. Cir. 2014). In a world increasingly marked by remote work, it is not unusual that companies like 1-800-Accountant, based in New York, would manage employees who work in Florida or other states and handle data that is physically stored on cloud servers in various locations around the country, and that is potentially accessible to job applicants or other users in countless other jurisdictions.

Despite these technological changes, to determine where venue is appropriate, we "must initially identify the conduct constituting the offense (the nature of the crime) and then discern the location of the commission of the criminal acts." *Rodriguez-Moreno*, 526 U.S. at 279. In performing this analysis, we must separate "essential conduct

elements" from "circumstance element[s]." *Id.* at 280 & n.4. Only essential conduct elements provide the basis for venue. To determine the nature of the offense, and which acts constitute "essential conduct elements," we must look to the relevant statutory language including, though not exclusively, the verbs the statute uses. *Id.* at 280.

Calonge was convicted under two subsections of the CFAA. The first criminalizes "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). The second criminalizes "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage." 18 U.S.C. § 1030(a)(5)(B). The statutory definition of "protected computer" includes, among other things, a computer that "is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). As the jury in this case was instructed, that definition essentially covers every computer connected to the Internet. *See United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015). Neither party disputes that Gaspari's computer was a protected computer. The jury was also instructed that "damage" under the CFAA covers "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

Each relevant subsection of the CFAA contains at least two essential conduct elements. The first, § 1030(a)(5)(A), bars (1) knowingly causing the transmission of a program and (2) intentionally causing damage. The second subsection bars (1) intentionally accessing and (2) recklessly causing damage. Venue is

thus appropriate in any place where Calonge transmitted the program, obtained access, or caused damage to a protected computer. The district court was therefore correct to instruct the jury that venue was appropriate in the Southern District of New York if Calonge damaged a protected computer within that district.

Calonge primarily argues that the government's evidence was insufficient to prove that a protected computer was damaged in the Southern District of New York. Calonge Br. at 18–32. We review sufficiency challenges *de novo*, and because Calonge was convicted after a jury trial, we "review the record evidence in the light most favorable to the government, drawing every reasonable inference in support of the jury's verdict." *United States v. Tang Yuk*, 885 F.3d 57, 71 (2d Cir. 2018).

We reject Calonge's arguments. Constitutionally sound venue existed in this case so long as the government established by a preponderance of the evidence that Gaspari's computer in the Southern District of New York was damaged by Calonge's conduct – in other words, that Calonge caused an "impairment" to the "availability of data" in the Southern District of New York. 18 U.S.C. § 1030(e)(8). At trial, Gaspari testified that when she logged into the JazzHR applicant tracking system from her computer in Manhattan, she saw that large amounts of data had been deleted and that she therefore no longer had access to the data. App'x at 157–58, 214. Drawing reasonable inferences in favor of the jury's verdict, we conclude that Gaspari's testimony that she was unable to access data stored in the JazzHR database from her computer in New York was sufficient to establish the only necessary fact for venue: that Calonge damaged a protected computer located in the Southern District of New York. There was no need for the government to prove that any

other employees' computers were damaged; one damaged computer was enough.[1]

Calonge argues that Gaspari's testimony is a "slender reed upon which to base venue given the uncontroverted, strong evidence that, in fact, it was JazzHR's servers in Virginia or California that were damaged." Calonge Br. at 25. But venue "may lie in more than one place if the acts constituting the crime and the nature of the crime charged implicate more than one location." *Tang Yuk*, 885 F.3d at 69 (quoting *United States v. Lange*, 834 F.3d 58, 68 (2d Cir. 2016)). Venue in the Southern District of New York could thus be appropriate even if venue would also have been appropriate in other districts.

Insofar as Calonge argues that deleting data from the JazzHR database did not damage any protected computer in New York, *see* Oral Argument Audio Recording at 33:52–34:10, we disagree. The text of the CFAA is clear that preventing a computer from accessing data

---

[1] We also note that Calonge could reasonably have foreseen being tried in New York, because she attempted to injure – and did injure – a computer operated in New York by a company headquartered there. In any event, Calonge has herself disavowed reliance on our "substantial contacts" test, which we have applied in other cases "in order to ensure that the policies and considerations underlying the Constitution's commands respecting venue have been preserved." *United States v. Saavedra*, 223 F.3d 85, 89 (2d Cir. 2000); *see also United States v. Davis*, 689 F.3d 179, 186 (2d Cir. 2012) (explaining that the substantial contacts test "asks whether the acts' occurrence in the district of venue would have been reasonably foreseeable to the defendant" (internal quotation marks and alterations omitted)). She emphasizes, correctly, that we apply that test only where "the defendant argues that his prosecution in the contested district will result in a hardship to him, prejudice to him, or undermine the fairness of his trial." *United States v. Rasheed*, 981 F.3d 187, 194–95 (2d Cir. 2020) (internal quotation marks omitted). Here, by her own account, Calonge has "never argued that the chosen venue was a hardship, prejudicial, or unfair to Ms. Calonge." Calonge Br. at 31.

that it regularly accesses constitutes "damage" under the statute. The statute defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The jury was entitled to conclude that Calonge's actions impaired the availability of data on the JazzHR system on Gaspari's computer. The fact that the deletion might also have damaged the Amazon servers located in Virginia and California makes no difference.

Finally, Calonge contends that *United States v. Auernheimer*, 748 F.3d 525 (3d. Cir. 2014) compels a different result. We are not persuaded. In that case, a hacker discovered a flaw in AT&T's security processes that allowed him to harvest the email addresses of iPad owners who used AT&T data services. *Id.* at 530–31. Auernheimer was charged with conspiracy to violate the CFAA, specifically, 18 U.S.C. § 1030(a)(2)(C), a subsection under which Calonge was *not* charged.[2] *Id.* at 531. Auernheimer was located in Arkansas, his coconspirator in California, and the servers that they accessed in Texas and Georgia. *Id.* Nevertheless, Auernheimer was prosecuted in New Jersey, where the government could charge him with a felony by alleging that his CFAA violation occurred in furtherance of a violation of New Jersey's computer crime statute. *Id.* The case's only connection to New Jersey was that some of the AT&T customers whose email addresses were harvested lived there.

The Third Circuit reversed Auernheimer's conviction. It held that the essential conduct elements of his offense did not involve New Jersey. The court concluded that the section of the CFAA that Auernheimer was charged with violating contained two essential

---

[2] 18 U.S.C. § 1030(a)(2)(C) criminalizes those who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer."

conduct elements: "*accessing* without authorization and *obtaining* information." *Id.* at 533 (emphasis in original). It then concluded that "New Jersey was not the site of either essential conduct element" and that "[n]o protected computer was accessed and no data was obtained in New Jersey." *Id.* at 534. Thus, the fact that the email addresses of some New Jersey residents were obtained from AT&T's servers was merely a "circumstance element" that could not support venue in New Jersey where the "essential conduct elements" of the crime all occurred in other states.

Applying the same analysis to the subsections of the CFAA that Calonge was convicted of violating, we reach the opposite conclusion. Here, unlike in *Auernheimer*, the essential conduct elements of Calonge's crime, specifically damaging a protected computer, occurred in the Southern District of New York. In fact, the Third Circuit anticipated this result when it expressly contrasted the provision of the CFAA under which Auernheimer was charged with the provision under which Calonge was charged, § 1030(a)(5)(B), and remarked that under § 1030(a)(5)(B), "venue could be proper wherever" damage was caused. *Auernheimer*, 748 F.3d at 537. Venue in the Southern District of New York was therefore appropriate.

III. CONCLUSION

For the foregoing reasons, the judgment of the District Court is **AFFIRMED.**