17-2479
United States v. Gasperini

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2017

(Argued: June 6, 2018 Decided: July 2, 2018)

Docket No. 17-2479-cr

UNITED STATES OF AMERICA,

Appellee,

— v. —

FABIO GASPERINI,

Defendant-Appellant.

B e f o r e :

CABRANES, LYNCH, and CARNEY, *Circuit Judges*.

Fabio Gasperini appeals from a judgment, entered after a jury trial in the United States District Court for the Eastern District of New York (Nicholas G. Garaufis, *Judge*), convicting him of misdemeanor computer intrusion in violation of 18 U.S.C. § 1030(a)(2)(C), and sentencing him to one year in prison. On appeal, Gasperini argues, among other things, that the computer intrusion statute is

unconstitutionally vague; that the district court erred in denying his motion to suppress evidence that was seized in purported violation of the Stored Communications Act; and that the district court abused its discretion in allowing the government to introduce into evidence screenshots from the Internet Archive. Because we find these arguments (and, as explained in an accompanying summary order, all of Gasperini's other arguments) to be meritless, we AFFIRM the judgment of the district court.

SARITHA KOMATIREDDY, Assistant United States Attorney (David C. James, Assistant United States Attorney, *on the brief*), *for* Richard P. Donoghue, United States Attorney for the Eastern District of New York, New York, NY.

SIMONE BERTOLLINI (Paul F. O'Reilly, *on the brief*), Law Offices of Simone Bertollini, New York, NY, *for* Defendant-Appellant Fabio Gasperini.

GERARD E. LYNCH, *Circuit Judge*:

Fabio Gasperini was convicted by a jury in the United States District Court for the Eastern District of New York (Nicholas G. Garaufis, *Judge*) of one count of misdemeanor computer intrusion in violation of 18 U.S.C. § 1030(a)(2)(C), a provision of the Computer Fraud and Abuse Act of 1986 ("CFAA"). Gasperini raises several challenges to his conviction. First, he contends that the statute that he was convicted of violating is unconstitutionally vague. Second, he asserts that the district court erroneously denied his motion to suppress evidence that was

allegedly collected in violation of the Stored Communications Act. Third, he contends that the district court abused its discretion in allowing the government to introduce into evidence screenshots from the Internet Archive (also known as the "Wayback Machine"). Gasperini makes several other arguments, which are addressed in an accompanying summary order. Because we are not persuaded by any of Gasperini's arguments, we AFFIRM the judgment of the district court.

BACKGROUND

The evidence discussed below is taken from the trial record. Insofar as it relates to the offense of conviction, the evidence is viewed in the light most favorable to the government, and we draw all reasonable inferences in its favor. *United States v. Guadagna*, 183 F.3d 122, 125 (2d Cir. 1999). As it relates to the sentencing issues discussed in the accompanying summary order, "we review the District Court's factual findings relevant to a sentencing determination for clear error." *United States v. Johnson*, 378 F.3d 230, 238 (2d Cir. 2004). In order to vacate such findings, "we must view the evidence in the light most favorable to the government and nevertheless find to be impermissible the factual determinations based upon that favorably-viewed evidence." *Id.*

In 2014, a virus began infecting QNAP-brand devices.[1] Computer security experts who detected the virus determined that the attacker behind the virus was attempting to covertly infiltrate computers. The attacker targeted QNAP computers, which do not log external internet connections, and used an often-overlooked port to access the computers. The virus installed malware, which included several commands for the computer to execute, in hidden directories on the infected computers. Once a computer was infected, the attacker installed a "backdoor" account, which had the status of a "superprivileged user," with unrestricted access to and control over the computer's data. After creating the backdoor account, the attacker patched the initial vulnerability that had allowed him access, thereby locking out other hackers. The infected computer was then instructed to scan the internet for other computers with the same vulnerability and infect them. In this way, the attacker created what is known as a "botnet" – a network of infected computers under the attacker's control. An analysis of one of the servers used in the scheme revealed that more than 155,000 computers were infected worldwide. Many of those computers were located in the United States.

[1] QNAP Incorporated is a company headquartered in Taiwan, with offices and warehouses in California, that manufactures and sells "network attached storages," which are computers specifically designed for the storage of data.

The virus's commands accomplished different tasks. One command was designed to take certain username and password files from the infected computers and copy them onto a server. Another caused the infected computer to disguise itself as a human browsing the internet, and to click on certain banner advertisements. Yet another command prompted the botnet to launch coordinated attacks on certain websites, a practice known as distributed denial-of-service attacks.

United States investigators identified Gasperini, an Italian citizen, as the creator of the virus and perpetrator of the various attacks because he leased and operated several servers around the world that were used to host the malware and communicate with the infected computers. A search of Gasperini's email account also found a "test" copy of the computer virus that was initially used to infect QNAP computers, and emails from Gasperini expressly referencing several of the scripts installed on the infected computers.

Evidence later adduced at trial also linked Gasperini to a related "click fraud" scheme, in which the botnet computers were commanded to click on certain advertisements. Business records showed that several websites implicated in the scheme were registered in Gasperini's name. Additionally, Gasperini

contracted with an Italian advertising company to earn money for each advertisement viewed on these websites. Finally, evidence at trial tended to show that Gasperini monitored the operation. This included emails from his servers reporting "clicks completed" and a photograph of his home computer commanding his botnet to click on an advertising banners. After his arrest in the Netherlands, Gasperini deleted the contents of his Google account, deactivated his Facebook account, and instructed someone to discard the hard drives in his home and erase others.

A grand jury charged Gasperini with felony crimes of computer intrusion with intent to defraud, for financial gain, and in furtherance of criminal acts; wire fraud conspiracy; wire fraud; and money laundering. After a seven-day jury trial, he was acquitted of all felony charges, and was convicted only of misdemeanor computer intrusion in violation of 18 U.S.C. § 1030(a)(2)(C), a lesser-included crime within one of the computer intrusion felonies charged in the indictment.[2] At sentencing, the trial judge found that the government had proven, by a preponderance of the evidence, that Gasperini had committed the felony offenses

[2] The misdemeanor offense lacks the aggravating purpose element of the felony charged in the indictment. *See* 18 U.S.C. § 1030(c)(2) (establishing escalating penalties for violations of § 1030(a)(2) under various circumstances).

with which he was charged. Accordingly, those crimes were considered as relevant conduct in calculating the applicable Guidelines range, resulting in a range of 63 to 78 months' incarceration, which was capped by the statutory maximum of imprisonment for one year. The district court sentenced Gasperini principally to that statutory maximum. He now appeals from that conviction.[3]

DISCUSSION

I. Vagueness

The statute under which Gasperini stands convicted punishes anyone who "intentionally accesses a computer without authorization . . . and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Gasperini argues that the statute is unconstitutionally vague because it does not define the terms "access," "authorization," and "information," and because the definition of "protected computer" in § 1030(e)(2) is overbroad.

Because Gasperini did not raise this challenge below, we review it for plain error. *United States v. Boyland*, 862 F.3d 279, 288 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 938 (2018). When reviewing for plain error under Federal Rule of Criminal Procedure 52(b), an appellate court has discretion to correct an error not raised at

[3] Gasperini has served his sentence and has been deported to Italy.

trial only where the appellant demonstrates that "(1) there is an error; (2) the error is clear or obvious . . . ; (3) the error affected the appellant's substantial rights . . . ; and (4) the error seriously affects the fairness, integrity[,] or public reputation of judicial proceedings." *United States v. Marcus*, 560 U.S. 258, 262 (2010) (internal quotation marks and brackets omitted).

Gasperini cannot clear the hurdle set by the second of these requirements. "At a minimum, a court of appeals cannot correct an error pursuant to Rule 52(b) unless the error is clear under current law." *United States v. Olano*, 507 U.S. 725, 734 (1993); *see also Rosales-Mireles v. United States*, 138 S.Ct. 1897 (2018). Gasperini cites no authority from *any* court – let alone one whose decisions are binding on us – holding, or even suggesting, that § 1030(a)(2)(C) is unconstitutionally vague. Accordingly, we cannot conclude that the district court plainly erred by not *sua sponte* dismissing the indictment on that ground.

In any event, Gasperini has not identified a due process violation here. "A conviction fails to comport with due process if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *United States v. Williams*, 553 U.S. 285, 304 (2008).

We apply this standard in the context of the facts at issue, because, outside of the First Amendment context, an individual "who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others." *Id*.

Even if we assume, *arguendo*, that the statute's application may be unclear in some marginal cases (including some fanciful possibilities conjured in Gasperini's appellate brief), Gasperini's conduct falls squarely and unambiguously within the core prohibition of the statute. "Congress enacted the CFAA in 1984 to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data." *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015), citing H.R. Rep. No. 98-894, at 3691–92, 3695–97 (1984), and S. Rep. No. 99-432, at 2480 (1986). In this case, Gasperini was found by the jury to have hacked into thousands of computers without permission, thereby gaining access to all of the information stored on those computers. The jury further found Gasperini guilty of taking information, including usernames and passwords, from at least some of those computers. There is thus no doubt that all of these actions fall within the core meaning of the phrase "*accesses* a computer without *authorization* . . . and thereby obtains . . .

information from [a] protected computer" as the italicized terms are used in § 1030(a)(2)(C).[4] Accordingly, Gasperini's challenge to the constitutionality of 18 U.S.C. § 1030(a)(2)(C) fails.

II. Suppression

Gasperini next argues that the district court should have suppressed certain evidence introduced by the government at trial, including (1) evidence obtained pursuant to search warrants issued under the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq*., and (2) evidence obtained during searches of his home in Italy by Italian law enforcement officers pursuant to warrants issued by Italian courts. The district court did not err with respect to either category of evidence.

Gasperini first argues that the SCA warrants were extraterritorial warrants not authorized by that Act. He relies on this Court's decision in *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), *vacated as moot sub nom. United States v. Microsoft Corp.*, 138

[4] Gasperini's questioning of the definition of "protected computer" is also meritless. The definition describes a wide range of computers, including ones "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). That standard, a familiar limitation on the reach of any number of federal criminal statutes, has never been found void for vagueness.

S. Ct. 1186 (2018), in which we held that the SCA does not apply extraterritorially, and does not authorize the seizure of electronic communications stored on servers located outside of the United States. *Id.* at 222.[5]

Even assuming that at least some of the warrants demanded and acquired electronic communications stored abroad,[6] and that our ruling in *Microsoft* –

---

[5] As we explained in *Microsoft*, SCA "warrants," although issued only when the constitutional standards governing conventional search warrants are met, do not authorize agents to enter premises and search for evidence, but rather are served on a third-party holder of electronic communications and demand that the third party turn over the information called for in the warrant. *See* 829 F.3d at 214 (describing the operation of SCA warrants). In that respect, SCA warrants function analogously to subpoenas. *See id*. at 226–29 (Lynch, *J*., concurring in the judgment).

[6] Gasperini asserts that because he lived in Italy, it is "obvious" that his emails and Google Drive files were stored in Google's foreign servers. Appellant's Br. at 36. That assertion is far from obvious, however. Prior to our decision in *Microsoft*, Google appears to have stored user data at locations that bore no relation to the location of the user. *See, e.g.*, *In re Search of Content that is Stored at Premises Controlled By Google*, No. 16-MC-80263-LB, 2017 WL 1398279, at *4 (N.D. Cal. Apr. 19, 2017) ("Unlike *Microsoft*, where storage of information was tethered to a user's reported location, there is no storage decision here. The process of distributing information is automatic, via an algorithm, and in aid of network efficiency") (internal citation omitted) (*amended and superseded on other grounds by In re Search of Content that is Stored at Premises Controlled by Google,* No. 16-MC-80263-LB, 2017 WL 1487625, at *1 (N.D. Cal. Apr. 25, 2017); *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708, 712 (E.D. Pa. 2017) ("Google stores user data in various locations, some of which are in the United States and some of which are in countries outside the United States. Some user files may be broken into component parts, and different parts of a single file may be stored in different

which was vacated as moot by the Supreme Court – correctly states the law, suppression still would not be required, because suppression of evidence is not a remedy available for violation of the SCA. Congress provided a number of specific remedies for such violations; these do not include suppression of evidence in a criminal case. *See* 18 U.S.C. § 2707(b) (listing "appropriate relief" in a "civil action" as "equitable or declaratory relief," "damages," and "a reasonable attorney's fee and other litigation costs reasonably incurred"); 18 U.S.C. § 2707(d) (providing for "disciplinary action against the officer or employee" who violated the Act). Moreover, Congress expressly provided that the listed remedies are *exclusive*, stating in § 2708 that the "remedies and sanctions described in this chapter are the *only* judicial remedies and sanctions for nonconstitutional violations of this chapter." (Emphasis added).[7] Gasperini does not request any

---

locations (and, accordingly, different countries) at the same time.") (internal citations omitted). Gasperini musters no evidence to support his conclusory assertion that in his case, the emails and files obtained from Google had, in fact, been stored abroad.

[7] Our reading of the SCA as not requiring or authorizing suppression of evidence for nonconstitutional violations of its provisions is consistent the rulings of our sister circuits that have considered the issue. *See*, *e.g.*, *United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011); *United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998); *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003).

form of relief authorized under the SCA, nor does he argue that any of the purported statutory violations he identifies also violate the Constitution, and we find no basis for any such argument. Accordingly, the district court did not err in denying Gasperini's motion to suppress the evidence collected pursuant to the SCA warrants.

Gasperini's challenge to the use of hard drives and documents obtained from Italian law enforcement officials who searched his home fares no better. The searches were conducted pursuant to an Italian warrant, and Gasperini makes no claim that the warrant was issued in violation of Italian law. He argues instead that the Italian officials acted at the behest of American law enforcement agents, thus making them subject to American constitutional requirements for searches. "In order to render foreign law enforcement officials virtual agents of the United States, American officials must play some role in controlling or directing the conduct of the foreign parallel investigation." *United States v. Getto*, 729 F.3d 221, 230 (2d Cir. 2013). Beyond alleging that the search was conducted at the request of the U.S. government, however, Gasperini does not argue that Italian officials were controlled by American law enforcement agents. A mere request is not sufficient to show control. *See, e.g.*, *id*. ("It is not enough that the foreign

government undertook its investigation pursuant to an American [Mutual Law Enforcement Assistance Treaty] request.") There is thus no basis for Gasperini's efforts to apply to the Italian searches the constitutional standards that would apply to domestic searches conducted by United States officers.

III. The Wayback Machine

Finally, Gasperini challenges an evidentiary ruling made by the district court permitting the government to introduce screenshots of various websites taken by the Internet Archive, more commonly known as the "Wayback Machine." "A district court judge is in the best position to evaluate the admissibility of offered evidence. For that reason, we will overturn a district court's ruling on admissibility only if there is a clear showing that the court abused its discretion or acted arbitrarily or irrationally." *United States v. Valdez*, 16 F.3d 1324, 1332 (2d Cir. 1994) (internal citation omitted). We detect no such abuse of discretion here.

Gasperini challenges the authentication of screenshots of websites registered to Gasperini for use in the click fraud scheme, which were captured and stored by the Internet Archive, and maintained as business records of that entity. Federal Rule of Evidence 901(a) requires that before evidence is admitted,

"the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." That standard was amply met here.

Gasperini relies on *Novak v. Tucows, Inc.*, 330 F.App'x 204 (2d Cir. 2009), in which we affirmed a district court decision excluding screenshots from the Archive for lack of authentication. In that non-precedential summary order, however, we held only that the district court did not abuse its discretion in excluding the evidence in a civil trial, where the proponent of the evidence offered no testimony explaining its provenance. *Id.* at 206, aff'g *Novak v. Tucows, Inc.*, No. 06-CV-1909, 2007 WL 922306 (E.D.N.Y. Mar. 26, 2007). Here, in contrast, the government presented testimony from the office manager of the Internet Archive, who explained how the Archive captures and preserves evidence of the contents of the internet at a given time. The witness also compared the screenshots sought to be admitted with true and accurate copies of the same websites maintained in the Internet Archive, and testified that the screenshots were authentic and accurate copies of the Archive's records. Based on this testimony, the district court found that the screenshots had been sufficiently authenticated.

The Third Circuit considered the admissibility of Internet Archive records on a similar record in *United States v. Bansal*, 663 F.3d 634, 667–68 (3d Cir. 2011). In that case, the court found that where a witness testified, from personal knowledge, "about how the Wayback Machine website works and how reliable its contents are," there was sufficient evidence to authenticate screenshots taken from that website. *Id.* at 667. We agree with the holding of the court in *Bansal*, and hold that the testimony presented in this case by the government was "sufficient proof . . . that a reasonable juror could find in favor of authenticity or identification." *United States v. Tin Yat Chin*, 371 F.3d 31, 38 (2d Cir. 2004). Gasperini was free to cross-examine the witness about the nature and reliability of the Archive's procedures for capturing and cataloguing the contents of the internet at particular times, and the jury was thus enabled to make its own decision about the weight, if any, to be given to the records. Accordingly, a sufficient basis was laid to place the admission of the evidence well within the discretion of the district court, and Gasperini's challenge therefore fails.

CONCLUSION

For the foregoing reasons, and those set forth in the accompanying summary order, we AFFIRM the judgment of the district court.