In the

United States Court of Appeals

For the Seventh Circuit

No. 14-1003

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

FRANK CAIRA,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division.
No. 08 CR 1052-1 — **Rebecca R. Pallmeyer**, *Judge.*

ARGUED FEBRUARY 11, 2016 — DECIDED AUGUST 17, 2016

Before RIPPLE, KANNE, and WILLIAMS, *Circuit Judges*.

WILLIAMS, *Circuit Judge*. Someone used the email address gslabs@hotmail.com to contact a Vietnamese website in an attempt to buy sassafras oil—a chemical that can be used to make the illegal drug known as ecstasy. The website was being monitored by the Drug Enforcement Administration, which began an investigation that culminated in Frank Caira

being convicted on drug charges. A key step in the investigation was learning that Caira was the person behind the gslabs@hotmail.com address. The DEA made that discovery by issuing administrative subpoenas to technology companies, without getting a warrant. Arguing that the DEA conducted an "unreasonable search" in violation of the Fourth Amendment, Caira moved to suppress much of the evidence against him. The district court denied his motion and we affirm. Because Caira voluntarily shared the relevant information with technology companies, he did not have a reasonable expectation of privacy in the information, so his Fourth Amendment rights were not violated.

In sentencing Caira, the district judge erred by imposing conditions of supervised release without justifying them on the record. But Caira is serving a life sentence for another conviction. He is not expected to be released from prison so the conditions are not expected to be imposed. If he *is* released, a court can modify the conditions at that point. So the judge's error was harmless and we affirm Caira's sentence as well.

I. BACKGROUND

Between July and September 2008, emails were sent from gslabs@hotmail.com to an email address associated with a website hosted in Vietnam. The emails asked about buying sassafras oil, an ingredient in ecstasy. The DEA, which had been monitoring the website, sent an administrative subpoena to Microsoft Corporation (the owner of Hotmail, the web-based email service for @hotmail.com email addresses). The subpoena asked for:

> [A]ll basic subscriber information, including the subscriber's name, address, length of service

> (including start date) and types of services used including any temporarily assigned network address, Passport.net accounts, means and source of payment (including credit card or bank account number), and the account login histories (IP Login history) of, the following email account(s): gslabs@hotmail.com.

For this case, the request for "account login histories (IP Login history)" is key. Internet Protocol (abbreviated as "I.P.") addresses are used to identify computers connected to the internet. The allocation of addresses is centrally managed so one can look up in a public registry which internet service provider "owns" a particular address.

Responding to the subpoena, Microsoft gave the DEA information about instances in which the gslabs@hotmail.com account was accessed between July 5 and September 15, 2008. For each instance, Microsoft provided the date, time, and an I.P. address associated with the computer that accessed the account. The DEA saw that 24.15.180.222 was an I.P. address frequently used to access the account, so it sent an administrative subpoena to Comcast Corporation (the owner of that I.P. address). The subpoena asked for:

> Any and all e-mail addresses associated with [24.15.180.222]; a) customer name and other user name(s); b) addresses; c) records of session times and durations; d) length of service (including start date) and types of service used; e) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and f) means and source of payment for such service

> (including any credit card or bank account numbers).

Comcast responded that the address was assigned to Anna Caira, and Comcast gave the DEA Anna's home address. The investigation continued from there and culminated in Anna's husband, Frank Caira, being charged with possessing and conspiring to manufacture illegal drugs, in violation of 21 U.S.C. sections 841(a)(1) and 846.

Caira moved to suppress evidence obtained through the subpoenas, arguing that the government's inquiry was a "search" under the Fourth Amendment, and that a warrant was required. The district court denied that motion and Caira pleaded guilty while reserving his right to appeal the denial of his suppression motion. This is that appeal. Caira also appeals his sentence because the district judge imposed conditions of supervised release without justifying the conditions on the record.

II. ANALYSIS

A. Caira Did Not Have a Reasonable Expectation of Privacy in His I.P. Addresses

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Caira contends that the DEA's actions amounted to an unreasonable search. The district court disagreed. We review the court's legal conclusions de novo, as well as its treatment of mixed questions of law and fact; we review its factual findings for clear error. *United States v. Henderson*, 748 F.3d 788, 790 (7th Cir. 2014).

Under the Fourth Amendment, a "search" occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *see Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Caira argues that I.P. addresses reveal information about a computer user's physical location, and people have both a subjective and objectively reasonable expectation of privacy in their physical location. But in *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court developed a bright-line application of the reasonable-expectation-of-privacy test that is relevant here. In what has come to be known as the "third-party doctrine," the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties … even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Smith*, 442 U.S. at 743–44 (citing *Miller*, 425 U.S. at 442–44).

In *Miller*, the defendant had no reasonable expectation of privacy in his banking records, even though they contained sensitive financial information, because he had voluntarily shared the information with a third party—the bank. 425 U.S. at 442–44. And in *Smith*, the defendant had no reasonable expectation of privacy in the phone numbers he dialed from his home phone because, as a necessary step in placing phone calls, he shared that information with the phone company. 442 U.S. at 743–44. Even if such defendants had a *subjective* expectation of privacy, *Miller* and *Smith* held that once information is voluntarily disclosed to a third party, any such expectation is "not one that society is prepared to recognize as reasona-

ble." *Smith*, 442 U.S. at 743 (internal quotation marks and citation omitted). Accordingly, the government's pursuit of the information "was not a 'search,' and no warrant was required." *Smith*, 442 U.S. at 746.

Caira complains about the DEA's inquiry into the I.P. addresses that were used to access gslabs@hotmail.com. In *United States v. Weast*, the Fifth Circuit wrote that I.P. addresses are broadcast "far and wide in the course of normal internet use." 811 F.3d 743, 747 (5th Cir. 2016). Caira has not argued that such a description is inaccurate; indeed, his lawyer appeared to concede as much at oral argument. In any event *Miller* and *Smith* control if Caira shared his I.P. address with even *one* third party. *See, e.g.*, *United States v. Christie*, 624 F.3d 558, 573–74 (3rd Cir. 2010) (because defendant shared his I.P. address with the websites he visited, the government did not need a warrant to obtain that address through the administrator of one of those websites); *United States v. Beckett*, 369 F. App'x 52, 56 (11th Cir. 2010) (nonprecedential) (defendant did not have a reasonable expectation of privacy in his I.P. address because that information is "transmitted during internet usage" and is "necessary for the [internet service providers] … to perform their services"); *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (defendant had no "Fourth Amendment privacy expectation" in his I.P. address, which he had shared with Yahoo! by using an online chat service); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (defendant had no reasonable expectation of privacy in the I.P. addresses of websites he visited, because he voluntarily shared that information with his internet service provider, as was necessary to view the websites).

Here, Caira shared his I.P. address with a third party—Microsoft. When he used his home computer and sent his username and password to Microsoft, he expected to see his Hotmail inbox displayed on his home computer screen. It would have done him no good if his inbox was instead displayed on the screen attached to his computer at work, or a computer at the public library, or the computer he used years earlier when first signing up for a Hotmail account. So every time he logged in, he sent Microsoft his I.P. address, specifically so that Microsoft could send back information to be displayed where Caira was physically present. So this case is controlled by *Miller* and *Smith*. *See Smith*, 442 U.S. at 742 ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."); *see also United States v. Graham*, 2016 U.S. App. LEXIS 9797, at *21 (4th Cir. May 31, 2016) (en banc) ("[L]ike the defendant in *Smith*, 442 U.S. at 745, Defendants here did 'assume the risk' that the phone company would make a record of the information necessary to accomplish the very tasks they paid the phone company to perform. They cannot now protest that providing this essential information was involuntary.").

This case parallels the Tenth Circuit's case in *United States v. Perrine*, 518 F.3d 1196. Here, law enforcement observed a suspicious conversation on Microsoft's email service. In *Perrine*, it was Yahoo!'s online chat service. *Id*. at 1199–1201. Here, the government sent a subpoena asking Microsoft for I.P. addresses associated with gslabs@hotmail.com. In *Perrine*, the subpoena asked Yahoo! for addresses associated with the username "stevedragonslayer." *Id*. at 1199. In each case, officials studied the subpoena response, focused on a particular

I.P. address, and sent a second subpoena, to the internet service provider that owned the address of interest (here, Comcast; in *Perrine*, Cox Communications). In each case, the response to that second subpoena led to the defendant's residence, which led to criminal charges against the defendant. *See Perrine*, 518 F.3d at 1199–1200. The *Perrine* court held that Perrine had no "Fourth Amendment privacy expectation" in the "information he gave to Yahoo! and Cox." *Id*. at 1204. A parallel conclusion here would require us to affirm the denial of Caira's motion to suppress.

But Caira urges reversal, arguing that his case is special because the DEA discovered the I.P. address associated with his home—and the DEA knew that would happen, because people often check their email from home—and the home is given special protection under the Fourth Amendment, *see Payton v. New York*, 445 U.S. 573, 586 (1986); *Kyllo*, 533 U.S. at 40. That argument is foreclosed by *Smith*, in which government officials sought information that they *knew* was connected to the defendant's home, and in which the Court explicitly rejected an argument identical to Caira's:

> Petitioner argues, however, that, whatever the expectations of telephone users in general, he demonstrated an expectation of privacy by his own conduct here, since he used the telephone *in his house* to the exclusion of all others. But the site of the call is immaterial for purposes of analysis in this case. Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless

> of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

442 U.S. at 743 (internal citations, quotation marks, and brackets omitted; emphasis in original).

Citing *United States v. Jones*, 132 S. Ct. 945 (2012), Caira next argues that his case is special because of the sheer volume of information collected by the DEA. In *Jones*, the Court held that "the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets," constituted a Fourth Amendment search. *Id*. at 948. Justice Scalia's lead opinion applied a framework that is not relevant here, *id*. at 949–54, but the concurring opinions addressed the relevant reasonable-expectation-of-privacy issue. Traditionally, a person had no reasonable expectation of privacy in his movements on public streets, so it would not be a "search" if officers watched him. *Id*. at 953 (citing *United States v. Knotts*, 460 U.S. 276, 281 (1983); *Kyllo*, 533 U.S. at 31–32). But two concurring opinions, signed by five Justices total, expressed the view that technology has changed the constitutional calculus by dramatically increasing the amount and precision of data that the government can easily collect. *Id*. at 955–56 (Sotomayor, J., concurring); 964 (Alito, J., concurring).

Jones concerned GPS tracking technology, which is not at issue here. Nonetheless, Caira argues that "the government was essentially given data that was equivalent to placing a

tracking device" on him. That is unhelpful exaggeration. In concluding that "longer term" use of GPS technology constitutes a Fourth Amendment search, *id*. at 955, 964, the *Jones* concurrences noted that such technology can monitor "every single movement," *id*. at 964, and so can reveal "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on," *id*. at 955 (quoting *People v. Weaver*, 12 N.Y.3d 433, 441–442 (N.Y. 2009)). But here, the government only received records of the I.P. addresses Caira used to log in to his Hotmail account. He did so from two unsurprising places: home and work. The government received no information about how he got from home to work, how long he stayed at either place, or where he was when he was *not* at home or work. On days when he did not log in, the government had no idea where he was. Plainly, the government had no "tracking device."

More fundamentally, *Jones* did not do away with the third-party doctrine. It had no occasion to, because the government used its own GPS device to track Jones's location—he had not shared his location with any third party. Caira criticizes the third-party doctrine and he is by no means alone in that criticism. Justice Sotomayor wrote that the doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id*. at 957; *see also Graham*, 2016 U.S. App. LEXIS 9797 at *39 ("[A]lthough the Court formulated the third-party doctrine as an articulation of the reasonable-expectation-of-privacy inquiry, it increasingly feels like an exception. A *per se* rule that it is unreasonable to expect privacy

in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy.").

The critique advanced by Caira, Justice Sotomayor, and others, is not new. It was made in both *Miller* and *Smith*—in dissent. *Miller*, 425 U.S. at 451 (Brennan, J., dissenting); *Smith*, 442 U.S. at 750 (Marshall, J., dissenting). So it is true that at least one Justice believes "it may be necessary" to reconsider the third-party doctrine. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). But it is also true that "[t]he Supreme Court has … twice rejected [Caira's critique]. Until the Court says otherwise, these holdings bind us." *Graham*, 2016 U.S. App. LEXIS 9797 at *27. Because Caira voluntarily shared his I.P. addresses with Microsoft, he had no reasonable expectation of privacy in those addresses. So the DEA committed no Fourth Amendment "search" when it subpoenaed that information, and the district court was right to deny Caira's motion to suppress.

B. Supervised Release Error Was Harmless

Caira also appealed his sentence. The district judge sentenced him to twenty-five years in prison, followed by five years of supervised release. The judgment specified fourteen conditions of supervised release, but those conditions were not justified on the record at Caira's sentencing hearing. Ordinarily, that would require us to remand for resentencing. *See United States v. Thompson*, 777 F.3d 368 (7th Cir. 2015); *United States v. Kappes*, 782 F.3d 828 (7th Cir. 2015); *United States v. Johnson*, 765 F.3d 702, 710–11 (7th Cir. 2014).

But Caira's case has a wrinkle. Before pleading guilty, in an attempt to avoid conviction, he tried to have the prosecutor and DEA agent murdered. For that, he was sentenced to life in prison. *See United States v. Caira*, 737 F.3d 455 (7th Cir. 2013).

Citing *United States v. Bour*, 804 F.3d 880, 887–88 (7th Cir. 2015), the government argues that the district judge's failure to justify the conditions of supervised release on the record was harmless because: (i) Caira will not be released from prison so he will not be subject to the conditions; and (ii) if for some reason he *is* released one day, a court can modify the conditions at that point, *see* 18 U.S.C. § 3583(e)(2). The government argues that such an approach is preferable because it avoids "perpetuating expensive and time-consuming appeals and resentencings." *Id*. at 888 (citing *United States v. Silvious*, 512 F.3d 364, 371 (7th Cir. 2008); *United States v. Tejeda*, 476 F.3d 471, 475 (7th Cir. 2007)). Caira did not respond to that argument in his reply brief, and we find it persuasive.

III. CONCLUSION

We AFFIRM the judgment of the district court.