United States Court of Appeals
For the First Circuit

No. 18-1407

UNITED STATES OF AMERICA,

Appellee,

v.

RUSTY HOOD,

Defendant, Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

[Hon. Nancy Torresen, U.S. District Judge]

Before

Barron, Circuit Judge,
Souter,* Associate Justice,
and Selya, Circuit Judge.

J. Hilary Billings, Assistant Federal Defender, for appellant.

Benjamin M. Block, Assistant U.S. Attorney, with whom Halsey B. Frank, United States Attorney, was on brief, for appellee.

April 3, 2019

*Hon. David H. Souter, Associate Justice (Ret.) of the Supreme Court of the United States, sitting by designation.

BARRON, **Circuit Judge**. Rusty Hood ("Hood") entered a conditional guilty plea in the District of Maine to transporting child pornography in violation of 18 U.S.C. § 2252A(a)(1). He now challenges his conviction and a condition of his supervised release. We affirm.

I.

On January 5, 2017, the Portland, Maine office of Homeland Security Investigations ("HSI") of the United States Department of Homeland Security received a call from the Cleveland, Ohio HSI office regarding an investigation into the transmission of child pornography via the smartphone messaging application Kik. According to the information gathered by the Cleveland office, an individual bearing the Kik username "rustyhood" had communicated with a Cleveland resident, Brian Keeling, regarding the exchange of child pornography and the sexual abuse of young children. The "rustyhood" Kik profile photograph was of a man holding a baby and wearing a sticker that indicated that he was a visitor at the Maine Medical Center.

The conversation log between the two men showed that, on May 16, 2016, "rustyhood" either sent or received what amounted to thirteen pornographic images of young children and bragged explicitly about his past sexual abuse of a neighbor's young daughter. The investigation also revealed that between May 15, 2016 and July 4, 2016, "rustyhood" had posted a total of six

pornographic images of children to a larger group chat as well as two links to files containing a total of fifty-eight photographs and eighteen videos of child pornography.

In response to this information, Portland HSI Agent David Fife ("Fife") issued an Emergency Disclosure Request ("EDR") -- a procedure authorized by the Stored Communications Act, 18 U.S.C. § 2702 -- to Kik requesting subscriber information and recent IP addresses associated with the "rustyhood" account. Kik responded that same day and provided Fife the date that the account was registered, the email address used to register the account, and the make and model of the device most recently used to access the account. Additionally, Kik provided Fife the most recent IP logs associated with the account, which indicated that someone had accessed the account from three separate IP addresses between December 7 and December 11 of 2016.

Based on the information acquired from Kik, Fife was able to determine independently that the three IP addresses belonged to the digital communications providers Metrocast Cable ("Metrocast") and Fairpoint Communications ("Fairpoint"). Utilizing an administrative summons procedure authorized by 18 U.S.C. § 2703, Fife requested from both companies the location information associated with those IP addresses. Metrocast and Fairpoint responded with information indicating that one of the IP

addresses was assigned to the Oakwood Inn in Sanford, Maine, while the other two addresses were linked to a residence there.

Through additional independent database searches that Fife undertook, he determined that there was only one individual in Maine with the name "Rusty Hood." This information led Fife to Hood's Facebook profile. The profile displayed an image that matched the image of the photograph attached to the "rustyhood" Kik account, included a link directing users to "chat with [him] on Kik" using the "rustyhood" username, and indicated that Hood lived in Sanford, Maine. Further investigation revealed that the Sanford Police Department had recently arrested a "Rusty Hood" and that his booking photograph matched the man depicted in both the Facebook and Kik profiles. Sanford Police also provided information indicating that Hood had been a guest in the Oakwood Inn at the same time the hotel's IP address was used to access Hood's Kik account.

Based on this information, on January 19, 2017, the government filed a criminal complaint that charged Hood with transporting child pornography in violation of 18 U.S.C. § 2252A(a)(1) and arrested Hood the next day. Hood was then indicted on March 1, 2017, for violations of both 18 U.S.C. § 2252A(a)(1) (transporting child pornography) and 18 U.S.C. § 2252A(a)(2) (receiving child pornography).

After his arrest, Hood filed a motion to suppress the evidence gathered from Kik, Metrocast, and Fairpoint pursuant to the EDR and the administrative summonses "as well as all evidence secured directly or indirectly as fruit of the evidence secured from the named entities." The motion did so on the ground that the government had violated the Fourth Amendment to the United States Constitution by acquiring the information at issue from these companies without a warrant. In response, the government invoked what is known as the third-party doctrine to argue that it was not required to obtain a warrant. The government explained that the third-party doctrine controlled here because the information that had been acquired from Kik, Metrocast, and Fairpoint, respectively, had been voluntarily disclosed to those companies, and thus any "fruit" from the acquisition of that information was not tainted. The District Court agreed with the government and rejected Hood's motion to suppress.

On January 29, 2018, Hood entered a conditional plea of guilty to the charge of transporting child pornography and reserved his right to appeal the District Court's denial of his motion to suppress. The judgment reflecting that guilty plea noted that the government had dismissed the second count of the indictment, which was for receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2).

Prior to sentencing, the United States Probation Office prepared a presentence report ("PSR") that recommended, in part, that Hood submit to periodic polygraph tests as a condition of his supervised release. Hood objected to this condition, arguing that the testing requirement violated his right against self-incrimination under the Fifth Amendment to the United States Constitution. The District Court disagreed, and, on April 26, 2018, sentenced Hood to 60 months' imprisonment followed by 10 years of supervised release, during which Hood would be subject to periodic polygraph testing.

On May 2, 2018, Hood filed a timely notice of appeal, in which he challenged the District Court's denial of his motion to suppress and thus his conviction, as well as the District Court's decision to impose periodic polygraph testing as a special condition of his supervised release. We turn now to those challenges.

II.

Hood moved to suppress "all evidence of any kind secured without a warrant" from Kik, Metrocast, and Fairpoint, including "his name, his email address, and the IP addresses," as well as "additional personal information," that Hood believed the companies also disclosed. On appeal, however, Hood appears to limit his challenge only to the District Court's conclusion that the government did not violate the Fourth Amendment in obtaining

from the companies and then reviewing the "specific IP addresses" associated with his Kik account, as well as the "specific dates and times associated with each instance of internet access accomplished from those IP addresses." We thus focus solely on that contention,[1] reviewing the District Court's factual findings for clear error and its legal conclusions de novo in considering Hood's challenge to the denial of his motion to suppress. See United States v. Scott, 566 F.3d 242, 245 (1st Cir. 2009).

The Fourth Amendment generally requires that the government obtain a warrant based on probable cause before conducting a search. See Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring) ("[U]nder the Fourth Amendment, warrants are the general rule."). For an "intrusion into [the] private sphere" to constitute a "search," a defendant must "seek[] to preserve something as private," and "society [must be] prepared to recognize [that privacy expectation] as reasonable." Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

[1] We note that Hood makes no argument that, insofar as the District Court correctly found that the government did not violate the Fourth Amendment in acquiring the information from Kik, it still erred in finding that the government did not violate the Fourth Amendment in acquiring any of the other information that he sought to suppress below. We thus treat any such argument as waived. See United States v. Zannino, 895 F.2d 1, 17 (1st Cir. 1990).

The government argues that the District Court correctly ruled that Hood lacked the requisite reasonable expectation of privacy in the information acquired from Kik under the so-called third-party doctrine. See Smith, 442 U.S. at 743-44 (noting that the Supreme Court has "consistently . . . held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties") Pursuant to that doctrine, the Supreme Court has separately held that the government need not obtain a warrant to obtain recordings of voluntary conversations surreptitiously captured via radio transmitter, see United States v. White, 401 U.S. 745, 752-53 (1971), records from banks, see United States v. Miller, 425 U.S. 435, 444 (1976), and certain phone call data from pen registers, see Smith, 442 U.S. at 745-46, because the information at issue in each instance had been voluntarily disclosed by the defendant to a third party, see id. at 743-44.

Hood does not dispute that he voluntarily disclosed the information to Kik that he now seeks to suppress. He contends, however, that the Supreme Court's recent decision in Carpenter shows that the third-party doctrine does not apply to the information at issue here and thus that the government needed a warrant to acquire that information.

In Carpenter, the defendant challenged on Fourth Amendment grounds the government's warrantless acquisition --

pursuant to 18 U.S.C. § 2703 -- of his cell-site location information ("CSLI") from his wireless telecommunications carrier that had been sent to cell towers by his cell phone and stored by that carrier. 138 S. Ct. at 2211-12. The CSLI data acquired in Carpenter depicted the defendant's movements across nearly 13,000 specific location points during a 127-day span. Id. at 2212.

The government, in response, invoked the third-party doctrine to justify its warrantless acquisition of the CSLI from the carrier. Id. at 2219. The Supreme Court held, however, that the government's acquisition of the CSLI from the carrier constituted a search, for which the government needed a warrant, because Carpenter retained a reasonable expectation of privacy in the CSLI at issue even though he had shared it with his wireless carrier. Id. at 2217-20.

Carpenter explained that, given the location information that CSLI conveyed and the fact that a cell phone user transmits it simply by possessing the cell phone, if the government could access the CSLI that it had acquired without a warrant in that case, then the result would be that "[o]nly the few without cell phones could escape" what would amount to "tireless and absolute surveillance." Id. at 2218. Carpenter thus declined to extend the third-party doctrine to the CSLI at issue in that case and instead determined that Carpenter did have a reasonable

expectation of privacy in the CSLI that he sought to suppress. Id. at 2219-20.

Hood contends that the IP address data that the government acquired from Kik without a warrant -- which concerned Hood's internet activity only on Kik and only over a four-day span -- is not materially different from the CSLI that was at issue in Carpenter. He notes in this regard that this information enabled Fife to determine Hood's precise location when he logged on to Kik, as well as the date and time of those digital transmissions. For that reason, he contends, Carpenter establishes that the government needed a warrant to acquire the information from Kik that he seeks to suppress, because "[t]he notion that anytime one accesses the internet from their cell phone, they are effectively providing the police a specific record of their whereabouts, is in direct contrast to society's expectations."

But, an internet user generates the IP address data that the government acquired from Kik in this case only by making the affirmative decision to access a website or application. By contrast, as the Supreme Court noted in Carpenter, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger. See id. at 2220. In fact, those pings are recorded every time a cell phone application updates of its own accord, possibly to refresh a news feed or generate new weather

data, id., such that even a cell phone sitting untouched in a suspect's pocket is continually chronicling that user's movements throughout the day.

Moreover, the IP address data that the government acquired from Kik does not itself convey any location information. The IP address data is merely a string of numbers associated with a device that had, at one time, accessed a wireless network. By contrast, CSLI itself reveals -- without any independent investigation -- the (at least approximate) location of the cell phone user who generates that data simply by possessing the phone. Id. at 2211-12.

Thus, the government's warrantless acquisition from Kik of the IP address data at issue here in no way gives rise to the unusual concern that the Supreme Court identified in Carpenter that, if the third-party doctrine were applied to the acquisition of months of Carpenter's CSLI, "[o]nly the few without cell phones could escape . . . tireless and absolute surveillance." Id. at 2218. Accordingly, we conclude that Hood did not have a reasonable expectation of privacy in the information that the government acquired from Kik without a warrant. This conclusion, moreover, is in accord not only with the rulings of all the circuits that had addressed this issue before Carpenter had been decided, see United States v. Caira, 833 F.3d 803, 806-08 (7th Cir. 2016); United States v. Wheelock, 772 F.3d 825, 828-29 (8th Cir. 2014);

United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500, 510-11 (9th Cir. 2008), but also with the ruling of the one circuit that has done so in the wake of Carpenter, see United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018).[2]

III.

We next address Hood's argument regarding the District Court's inclusion of periodic polygraph testing as a special condition of his supervised release. We review the imposition of special conditions for supervised release under the abuse-of-discretion standard. United States v. Smith, 436 F.3d 307, 310 (1st Cir. 2006). Under that standard, we review purely legal questions de novo, factual issues for clear error, and "judgment calls" through a "classically deferential" lens. Riva v. Ficco, 615 F.3d 35, 40 (1st Cir. 2010).

Hood argues that the polygraph testing condition facially violates his Fifth Amendment right against self-incrimination, because it forces him either to answer potentially

[2] Given that Carpenter does not provide a basis for making an exception to the third-party doctrine with respect to the government's acquisition from Kik of the IP address data that Hood seeks to suppress, we need not address his separate challenge to the District Court's denial of his request for an evidentiary hearing on whether, under Carpenter, he has a reasonable expectation of privacy in that information.

incriminating polygraph questions truthfully or to have his supervised release revoked. He relies for this assertion on Minnesota v. Murphy, which provides that the Fifth Amendment "privileges [individuals] not to answer official questions put to [them] in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate [them] in future criminal proceedings." 465 U.S. 420, 426 (1984) (quoting Lefkowitz v. Turley, 414 U.S. 70, 77 (1973)). But, we agree with the government that our decision in United States v. York, 357 F.3d 14, 25 (1st Cir. 2004), requires us to reject this facial challenge to the condition of supervised release at issue.

The condition that Hood challenges requires that he "submit to periodic random polygraph examinations as directed by the probation officer to assist in treatment and/or case planning related to behaviors potentially associated with sex offense conduct." The condition also contains limiting language, however. That limiting language states, in relevant part: "[n]o violation proceedings will arise solely on the defendant[’s] failure to pass a polygraph examination, or on the defendant’s refusal to answer polygraph questions based on 5th amendment grounds. Such an event could, however, generate a separate investigation."

Insofar as this limiting language ensures that "[n]o violation proceedings will arise . . . on the defendant's refusal to answer polygraph questions," the condition is not materially

different from the one that we upheld in York against a similar, Fifth Amendment-based facial challenge. Id. There, the relevant limiting language in the condition stated that "[w]hen submitting to a polygraph exam, the defendant does not give up his Fifth Amendment rights." Id.

We concluded in York that, although such limiting language was not entirely clear in terms of the protection that it affords a defendant from being penalized for refusing to answer a polygraph question, it comfortably could be construed to ensure that a refusal to answer a question cannot supply a basis for a violation proceeding. Id. That is no less true here. If anything, the condition at issue in this case is more explicit in its assurance that "the defendant's refusal to answer polygraph questions based on 5th amendment grounds" will not be used as the basis for a violation proceeding.

Moreover, we noted in York that the government had urged us to adopt this Fifth Amendment-protective construction of the condition's limiting language. Id. The government similarly argues here that the condition's "plain language" demonstrates that no revocation of supervised release would occur due to an invocation of Hood's Fifth Amendment privilege.

Thus, we follow the government's lead here -- just as we did in York. Accordingly, we construe this condition to be just

as protective of the defendant's Fifth Amendment rights as the condition that we upheld in York.

Hood does point out that the word "solely" appears in the text of the condition's limiting language, and it is true that the limiting language that we considered in York did not contain either that qualifying word or an equivalent one. Nevertheless, the word "solely" need not be read to modify both the "defendant's failure to pass a polygraph examination" and the "defendant's refusal to answer polygraph questions based on 5th amendment grounds." If the word is read to modify only the former phrase, then it provides no basis for construing the condition to suggest that Hood's refusal to answer a polygraph question may be relied upon in a decision to initiate violation proceedings against him. We thus do not read the word "solely" to apply to the portion of the limiting language that is akin to the limiting language that was present in the condition at issue in York. As a result, the appearance of the word "solely" in the condition's limiting language provides no basis for distinguishing York.[3]

[3] We note that Hood makes no argument that the portion of the condition's limiting language that states that "[s]uch an event could . . . generate a separate investigation" provides a basis for reaching a different conclusion from the one that we reached in York. Nor do we see how that portion could, given that it does not make clear what set of circumstances would prompt such an investigation, what that investigation would entail, or what consequences might arise from such an investigation.

Hood separately contends that, even if the polygraph condition is not facially unconstitutional, it is unconstitutional as applied to him due to his limited mental ability and the absence of any requirement that he be warned, in compliance with the Supreme Court's decision in Miranda v. Arizona, of his constitutional rights before he is subjected to polygraph questioning. 384 U.S. 436, 467-74 (1966). But, this as-applied, Fifth Amendment-based challenge necessarily depends on future factual contingencies. For that reason, it, unlike the facial challenge to the condition that we have rejected on the merits, is not ripe for our review. Cf. United States v. Medina, 779 F.3d 55, 67 (1st Cir. 2015); United States v. Sebastian, 612 F.3d 47, 52 (1st Cir. 2010); York, 357 F.3d at 25; see also United States v. Rojas-Tapia, 446 F.3d 1, 7 (1st Cir. 2006) (holding that low mental acuity cannot, without evidence of actual coercion, suffice to prove that a Fifth Amendment violation occurred).

IV.

For the forgoing reasons, we **affirm** the District Court's decision as to both Hood's motion to suppress and the condition of his supervised release.