[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-15611

D.C. Docket No. 2:17-cr-14047-DMM-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

SCOTT JOSEPH TRADER,

Defendant-Appellant.

Appeals from the United States District Court
for the Southern District of Florida

(November 25, 2020)

Before WILLIAM PRYOR, Chief Judge, HULL and MARCUS, Circuit Judges.

WILLIAM PRYOR, Chief Judge:

This appeal requires us to decide whether the government needed a warrant to obtain a criminal suspect's email address and internet protocol addresses from a third party's business records. It also requires us to decide whether probable cause supported a warrant to search the defendant's house and whether a sentence of life imprisonment was an unreasonable punishment for his crimes involving child

pornography. We conclude that the government did not need a warrant for the third party's business records, probable cause supported the warrant to search the defendant's house, and the sentence was reasonable. We affirm.

I. BACKGROUND

For years, Scott Trader recorded videos of himself sexually abusing his daughters and distributed the videos on the internet. The abuse occurred while one daughter was a preteen and the other was a toddler. When abusing his own children was not enough, Trader used messaging apps to send child pornography to other young girls and to solicit nude photos and videos from them. He exchanged child pornography with more than forty minors and engaged in sexually explicit conversations with more than a hundred apparent minors. And he took other opportunities when they presented themselves, like recording a video of himself exposing his daughter's young friend during a sleepover.

Trader came to the attention of the Department of Homeland Security on May 30, 2017, when a parent in North Carolina discovered that someone had sent his nine-year-old daughter child pornography and solicited nude photos from her. The conversation occurred on an app called SayHi, and the perpetrator's username was "Scott." The parent reported the conversation to his local police department, which referred the report to Homeland Security.

Homeland Security agents examined the nine-year-old's device and learned that "Scott" sent her a sexually explicit video that he said depicted himself and his daughter. He also sent a photo of his face. The agents observed that Scott's profile on SayHi disclosed his username on another messaging app, Kik. The associated Kik profile photo matched the photos of "Scott" on SayHi.

The investigation unfolded quickly. Because SayHi was based abroad but Kik was domestic, agents thought Kik would be more responsive to requests for information about the user. The agents sent Kik an emergency disclosure request seeking information about the user. Kik provided the user's email address and recently used internet protocol addresses. The email address associated with the account was "strader0227@yahoo.com." And the user had repeatedly logged into Kik from a cell phone using a particular internet protocol address over the last month.

Homeland Security next traced the internet protocol address to the internet service provider, Comcast. Agents sent Comcast an emergency disclosure request for the subscriber records associated with the repeated internet protocol address. Comcast obliged. The account was registered to Shelly Trader and located at an address on Edinburgh Drive in Port St. Lucie, Florida.

State records revealed that a person named Scott Trader had a driver's license associated with the mailing address, and his driver's license photo matched

the photos from SayHi and Kik. A criminal records check revealed that Trader had been charged in December 2016 with molesting a victim younger than 12. And property records revealed that Shelly Trader-Bonanno and Leon Bonanno owned the Edinburgh Drive house, and Trader-Bonanno's age was consistent with her being Trader's mother.

Homeland Security used that information to apply for a warrant to search the Edinburgh Drive house. The warrant affidavit recited the steps of the investigation. It explained that "there were logons to the [Kik] account from" the internet protocol address associated with Trader's residence "starting 1 May 2017, through 31 May 2017, at 06:36 UTC." The warrant affidavit also explained that child pornography distributors and collectors "almost always possess and maintain their material . . . in the privacy and security of their homes" and that traces of child pornography could likely be found through forensic examination of devices that had been used to access child pornography.

A federal magistrate judge issued the warrant shortly before midnight on May 31. Law enforcement executed the warrant that same night. They found a stash of electronic devices hidden behind a loose board under a storage cabinet in Trader's bedroom. Forensic examination of the devices revealed years' worth of videos of Trader sexually abusing his daughters, along with thousands of images and videos of child pornography Trader had downloaded from the internet, plus

archived messages in which Trader shared child pornography with others and solicited nude images and videos from young girls. The devices also contained conversations in which Trader described in graphic detail his abuse of his daughters and his plans to escalate that abuse in the future. He also encouraged two women to ignore their feelings of guilt, participate in abusing his daughters, and abuse their own daughters.

Officers arrested Trader. A grand jury indicted him for enticing a minor to engage in sexual activity, enticing a minor to produce a sexually explicit video, and possessing and distributing child pornography. 18 U.S.C. §§ 2251(a), (e); 2252(a)(2), (a)(4)(B), (b)(1)–(2); 2256(2); 2422(b). Trader moved to suppress the evidence from Kik and from the search of the Edinburgh Drive house. The district court denied the motion. Trader pleaded guilty to all the charges on the condition that he retained the right to appeal the denial of the motion to suppress and could withdraw his guilty plea if he succeeded on appeal.

The presentence report detailed that Trader had been caught engaging in similar behavior before. He was charged in 2012 with promoting a sexual performance by a child, possessing child pornography, and lewd behavior after a police officer discovered a stash of child pornography on Trader's laptop computer. But the more serious charges were dismissed, and Trader eventually pleaded no contest to felony child neglect. In December 2016, he was charged with

molesting a victim younger than 12. That charge arose out of a September 2016 report by Trader's older daughter that Trader was molesting her. But Trader managed to keep custody of his daughters, and he continued to abuse them and collect child pornography while he was on bond awaiting prosecution for that crime.

At the sentencing hearing, the government played several pornographic videos of his daughters that Trader created. The government also played child pornography videos Trader had downloaded that involved sadomasochistic conduct, abuse of toddlers, and bestiality. The prosecutor summed up the rest of Trader's library of child pornography as containing "the most disturbing things that the [case] agent and I have ever seen." And the government played a recorded jail call during which Trader promised to kill the mother of one of his daughters if released. Last, the government presented the testimony of the mothers of Trader's daughters. Both women described the effects of Trader's abuse on the girls, and both asked the judge to impose a life sentence.

For his part, Trader presented the testimony of a forensic psychologist who explained that Trader was a pedophile who would always want to abuse children, but that he would have a low risk of abusing children if he received therapy in prison and was not released until age 60. The psychologist admitted that he was not aware that Trader continued molesting his daughters and downloading child

pornography while on probation and bond, that he had over 100 victims, or that he threatened to dox his young victims if they did not continue sending him images. And he admitted that some of those facts raised the likelihood that Trader would reoffend. Relying on the psychologist's testimony, Trader asked for a 28-year sentence so that he would be released at age 60.

Trader's base offense level was 32, based on section 2G2.1 of the United States Sentencing Guidelines. He received two-level enhancements for distribution, commission of a sexual act or sexual contact, and being a parent of a minor involved in the offense; four-level enhancements for depicting an infant or toddler or sadistic or masochistic content and for having victims younger than 12; and a five-level enhancement for a pattern of behavior. He received a three-level reduction for acceptance of responsibility, producing an offense level of 48, which the guidelines treat as the maximum offense level of 43. His criminal history category was III, so his guideline-sentencing range was life imprisonment.

The district court sentenced Trader to life imprisonment for enticing a minor to engage in sexual activity, along with concurrent sentences of 240 months each for possessing and distributing child pornography and 360 months each for two counts of producing child pornography. The district court explained that it had "considered the advisory guidelines as well as the statutory factors and the arguments of Counsel." It viewed the most important statutory factors as the

"serious nature of the offense," "the characteristics of the offender," and "the need to protect the public." The district court expressed "no confidence that [Trader] will stop" abusing children and obtaining and distributing child pornography "because he continued it while on bond from a state court proceeding and even while he was being evaluated by medical professionals[.]" It "t[ook] seriously" but rejected Trader's argument that he would not reoffend if he were released at age 60. And it mentioned Trader's threat to kill his ex-wife. "[F]or all of those reasons," the district court sentenced Trader to life imprisonment.

II. STANDARDS OF REVIEW

In an appeal of the denial of a motion to suppress, we review findings of fact for clear error and view the evidence in the light most favorable to the prevailing party, and we review the application of the law *de novo*. *United States v. Gibson*, 708 F.3d 1256, 1274 (11th Cir. 2013). We give great deference to a determination of probable cause. *United States v. Shabazz*, 887 F.3d 1204, 1214 (11th Cir. 2018).

We review the reasonableness of a sentence for abuse of discretion. *Gibson*, 708 F.3d at 1275. The party challenging the sentence bears the burden of proving that the sentence was unreasonable, and it succeeds if it shows that the district court failed to consider relevant factors that were due significant weight, gave significant weight to an improper or irrelevant factor, or made a clear error of judgment in balancing the applicable factors. 18 U.S.C. § 3553(a); *United States v.*

Kuhlman, 711 F.3d 1321, 1326–27 (11th Cir. 2013); *United States v. Tome*, 611 F.3d 1371, 1378 (11th Cir. 2010).

III. DISCUSSION

Trader appeals the denial of his motion to suppress the information from Kik and from the search of the Edinburgh Drive house, and he challenges his sentence as unreasonable. We address each issue in turn.

A. Carpenter *Did Not Create a Reasonable Expectation of Privacy in Email Addresses or Internet Protocol Addresses*.

The Fourth Amendment provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ." U.S. Const. amend. IV. A search occurs for the purposes of the Fourth Amendment "when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Ordinarily, a person lacks a reasonable expectation of privacy in information he has voluntarily disclosed to a third party. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). This principle is called the third-party doctrine.

While Trader's appeal was pending, the Supreme Court held that the third-party doctrine does not apply to retrospective collection of cell-site location information for periods of at least seven days. *Carpenter v. United States*, 138 S.

Ct. 2206, 2217 & n.3 (2018). Cell-site location information is the record created every time a cell phone transmits or receives data through a cell tower. *Id.* at 2211. The accuracy of the data "is rapidly approaching GPS-level precision." *Id.* at 2219. Many cell sites can "pinpoint a phone's location within 50 meters." *Id.* And cell phone users do not share their cell-site location information voluntarily: Carrying a cell phone is "indispensable to participation in modern society," cell phones generate cell-site location information "without any affirmative act on the part of the user," and users have no way to stop data collection other than making the phone useless by disconnecting it from the network. *Id.* at 2220.

Absent *Carpenter*, the third-party doctrine would undoubtedly apply to the information the government received from Kik. Trader affirmatively and voluntarily acted to download Kik onto his phone and to create an account on the app. He conveyed his internet protocol address and email address to a third party when he logged into Kik. And he did so voluntarily, affirmatively acting to open the app and log in, and without taking available steps to avoid disclosing his internet protocol address. *See United States v. Taylor*, 935 F.3d 1279, 1282, 1284 n.4 (11th Cir. 2019) (recognizing a reasonable expectation of privacy in internet protocol addresses of individuals who used software to avoid disclosing their internet protocol addresses). So the government violated the Fourth Amendment only if *Carpenter*'s exception to the third-party doctrine applies.

The third-party doctrine controls here because *Carpenter*'s "narrow" exception, *Carpenter*, 138 S. Ct. at 2220, applies only to some cell-site location information, not to ordinary business records like email addresses and internet protocol addresses. In *Carpenter*, the Court said, "we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI [cell-site location information]." *Id.* at 2217; *see also United States v. Gayden*, 977 F.3d 1146, 1151 (11th Cir. 2020) ("[T]he Supreme Court in *Carpenter* declined to extend the third-party doctrine to cell-site location information . . . ."); *United States v. Green*, 969 F.3d 1194, 1206 (11th Cir. 2020) ("The Supreme Court recently held in *Carpenter* . . . that the acquisition of historical cell-site records is a search under the Fourth Amendment, so the government must obtain a warrant to access such records."). *Carpenter* did not decide even whether cell-site location information always falls outside the third-party doctrine's reach. It left open the possibility that the government could obtain less than seven days' worth of cell-site location information without a warrant. *Carpenter*, 138 S. Ct. at 2217 n.3. It likewise left open the possibility that the government could collect cell-site location information in real time or through "tower dumps" not focused on a single suspect. *Id.* at 2220. And the Court made clear that it did not address "other business records that might incidentally reveal location information." *Id.* The Court "d[id] not express a view on matters not

before [it]," lest it "embarrass the future." *Id.* (internal quotation marks omitted). Indisputably, email addresses and internet protocol addresses were not at issue in *Carpenter*. The third-party doctrine applies, so the government did not need a warrant to obtain Trader's email address or internet protocol addresses from Kik.

Our sister circuits agree. Before *Carpenter*, every circuit to consider this issue decided that subscriber information disclosed during ordinary use of the internet, including internet protocol addresses and email addresses, falls within the third-party doctrine. *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (collecting decisions); *see also United States v. Christie*, 624 F.3d 558, 573–74 (3d Cir. 2010); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010); *United States v. Weast*, 811 F.3d 743, 747–48 (5th Cir. 2016); *United States v. Caira*, 833 F.3d 803, 806–09 (7th Cir. 2016); *United States v. Wheelock*, 772 F.3d 825, 828–29 (8th Cir. 2014). And every circuit to consider the question after *Carpenter* has reached the same conclusion. *United States v. Morel*, 922 F.3d 1, 9 (1st Cir. 2019); *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018); *see also United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. 2019); *United States v. VanDyck*, 776 F. App'x 495, 496 (9th Cir. 2019).

Despite the Court's clear language limiting the reach of its decision, Trader argues that *Carpenter* applies because his email address and internet protocol addresses constitute "cell phone location records." *Carpenter*, 138 S. Ct. at 2217.

But that argument not only misunderstands *Carpenter*'s holding; it also fails on its own terms because email addresses and internet protocol addresses are neither location records nor cell phone records.

Neither kind of information directly records an individual's location. An internet protocol address is a string of characters associated in an internet provider's business records with a particular device connecting to the internet through a particular network. *See United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019). Internet protocol addresses can be translated into location information only indirectly, by examining the internet company's business records to determine the physical address where the network is registered. *Id.* This kind of "business record[] that might incidentally reveal location information" falls outside *Carpenter*'s narrow exception to the third-party doctrine. *Carpenter*, 138 S. Ct. at 2220. As for email addresses, Trader does not even attempt to explain how they could be considered location records.

Neither kind of information is more than incidentally associated with cell phones. Many kinds of devices access wireless internet networks: computers, tablets, gaming consoles, household appliances, and more. *See Mozilla Corp. v. FCC*, 940 F.3d 1, 39 (D.C. Cir. 2019). And each of those devices has an internet protocol address. *Id.* We cannot conclude that internet protocol addresses are cell phone records when they are a feature of every electronic device that connects to

the internet. Some individuals may use cell phones to send and receive emails, but it strains credulity to say that use transforms email addresses into cell phone records. Even Trader does not claim that much.

Trader bases some of his arguments on information outside the record about the request for subscriber information Homeland Security sent Kik and the response from Kik. We do not consider that information because it is outside the record. Fed. R. App. P. 10. And we do not consider the arguments Trader raises for the first time in his reply brief based on *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Karo*, 468 U.S. 705 (1984); and *Kyllo v. United States*, 533 U.S. 27 (2001). *See Jones v. Sec'y, Dep't of Corrs.*, 607 F.3d 1346, 1353–54 (11th Cir. 2010).

B. Probable Cause Supported the Warrant to Search Trader's House.

The Fourth Amendment required the government to have probable cause for the warrant to search Trader's home. U.S. Const. amend. IV. Probable cause exists if, "given all the circumstances set forth in the affidavit . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). To establish probable cause to search a home, a warrant affidavit must "establish a connection between the defendant and the residence to be searched and a link between the residence and

any criminal activity." *United States v. Martin*, 297 F.3d 1308, 1314 (11th Cir. 2002).

The warrant application provided more than enough evidence to establish a fair probability that the Edinburgh Drive house contained evidence that a crime had been committed. Recall the investigation: A SayHi user with the username "Scott" distributed child pornography and solicited its creation on the evening of May 30. That user's profile linked to a profile on Kik. The Kik and SayHi profile photos and a photo "Scott" sent on SayHi matched each other. The Kik user's email address was "strader0227@yahoo.com." The Kik user logged into Kik from a particular internet protocol address either on the day of the crime—May 30—or within a few hours afterwards, early on the morning of May 31. That internet protocol address was registered to Shelly Trader at the Edinburgh Drive house. Scott Trader's driver's license photo matched the Kik and SayHi photos, and he listed the Edinburgh Drive house as his mailing address. Child pornographers typically keep stashes of child pornography in their houses. And traces of child pornography typically remain present on electronic devices long after files are downloaded or sent. That evidence is more than enough to establish probable cause.

Trader argues that probable cause did not support the warrant because the affidavit established a connection only between a Kik user and the Edinburgh

Drive house, not between the SayHi user and the Edinburgh Drive house. He argues that the warrant depended "simply on a hunch that Mr. Trader was the user of both applications." We disagree.

Trader would have us separately consider each fact and ignore the interrelationship of the evidence supporting the warrant. Probable cause does not work that way. Together, the matching images from SayHi, Kik, and Trader's driver's license, and the SayHi account's reference to the Kik account, established more than a fair probability that the user of both SayHi and Kik was Scott Trader.

Trader also argues that the district court misread the warrant affidavit as stating that Trader accessed Kik from the internet protocol address associated with the Edinburgh Drive house on the same day he sexted with the nine-year-old victim, May 30. But we need not delve into that issue. Even if Trader were correct, that minor mistake would not affect our conclusion that ample probable cause supported the warrant.

Trader last argues that the warrant affidavit failed to establish a connection between Trader and the Edinburgh Drive residence. But again we disagree. The affidavit established that Trader listed the Edinburgh Drive house as his mailing address, that he had access to its internet network, that the house's owner shared his last name and was about the age his mother would be, and that he connected to the internet network within a few hours of exchanging child pornography with a

nine-year-old girl. That evidence establishes more than a fair probability that Trader had a connection to the house, especially under the deferential standard of review that applies to a probable-cause determination. *Gibson*, 708 F.3d at 1274; *Shabazz*, 887 F.3d at 1214. And because probable cause existed, we need not address the alternative argument that the good-faith exception applies. *See United States v. Leon*, 468 U.S. 897, 922 (1984).

C. Trader's Life Sentence Is Reasonable.

Finally, Trader argues that his sentence of life imprisonment is substantively unreasonable. He says the district court gave undue weight to the guidelines and too little weight to his redeeming personal qualities. We disagree.

The district court imposed a reasonable sentence. After it acknowledged the advisory nature of the guidelines, the district court explained the statutory factors it found most important: the nature of the offense, the characteristics of the offender, and the need to protect the public. 18 U.S.C. § 3553(a)(1), (a)(2)(C). The parties' evidence and arguments throughout the sentencing hearing focused on precisely those issues, especially the risk of recidivism. The evidence established that Trader had over 100 victims; repeatedly sexually abused his daughters, recorded the incidents, shared them on the internet, and planned to continue and escalate his abuse in the future; continued this behavior despite an earlier conviction for it, a pending prosecution for it, and court supervision for it; encouraged others to abuse

their own daughters; and possessed a cache of the most disturbing child pornography the prosecutor and case agent had ever seen. On this record, the district court did not abuse its discretion by imposing a within-guidelines sentence of life.

Trader unpersuasively argues that his sentence is too harsh in the light of his age, family ties, lack of serious criminal history, contributions to the community, and cooperation with authorities. It is unclear what his age—32, at the time of sentencing—and his unspecified contributions to the community should change about the sentencing decision. And Trader's criminal history cuts against him because a short prison sentence had already failed to deter him from his behavior. To be sure, Trader's family ties and cooperation with authorities are mitigating factors: he lived with his mother, father, stepfather, and autistic brother, and his mother reported that they had a positive relationship. And Trader pleaded guilty promptly after his motion to suppress was denied. But the district court considered those mitigating factors and concluded that, on balance, Trader still deserved a life sentence. That conclusion was no abuse of discretion.

Trader next argues that the district court should not have relied on the child pornography sentencing guidelines because they are excessively punitive, but his arguments miss the mark. For example, he criticizes section 2G2.2 of the guidelines, which applies to child pornography *distribution* offenses, even though

his sentence was based on section 2G2.1, which applies to child pornography *production* offenses. And he argues that the child pornography guidelines are excessive compared to other guidelines because his offense level, inclusive of enhancements, is higher than the base offense level, without enhancements, for first-degree murder. But that apples-to-oranges comparison makes no sense. The district court did not impose an unreasonable sentence by considering the advisory guidelines in determining Trader's sentence.

IV. CONCLUSION

We **AFFIRM** Trader's conviction and sentence.