APPENDIX

APPENDIX

A-1

[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.

A-20

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-15611-DD

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

SCOTT JOSEPH TRADER,

Defendant - Appellant.

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

ON PETITION(S) FOR REHEARING AND PETITION(S) FOR REHEARING EN BANC

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

PER CURIAM:

The Petition for Rehearing En Banc is DENIED, no judge in regular active service on the Court having requested that the Court be polled on rehearing en banc. (FRAP 35) The Petition for Rehearing En Banc is also treated as a Petition for Rehearing before the panel and is DENIED. (FRAP 35, IOP2)

ORD-42

A-21

NO. 17-15611-DD

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff/appellee,

v.

SCOTT JOSEPH TRADER,
Defendant/appellant.

On Appeal from the United States District Court
For the Southern District of Florida

PETITION FOR REHEARING EN BANC OF THE APPELLANT SCOTT JOSEPH TRADER

MICHAEL CARUSO
Federal Public Defender

Fletcher Peacock
Assistant Federal Public Defender
Attorney for Appellant Trader
109 North 2nd Street
Fort Pierce, Florida 34950
Tel. (772) 489-2123

THIS CASE IS ENTITLED TO PREFERENCE
(CRIMINAL APPEAL)

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

United States v. Scott Joseph Trader
Case No. 17-15611-BB

Appellant files this Certificate of Interested Persons and Corporate Disclosure Statement, listing the parties and entities interested in this appeal, as required by 11th Cir. R. 26.1.

Barnes, Antonia J., Assistant United States Attorney

Cannon, Aileen M., United States District Judge

Former Assistant United States Attorney

Caruso, Michael, Federal Public Defender

Fajardo Orshan, Ariana, United States Attorney

Ferrer, Wifredo A., Former United States Attorney

Greenberg, Benjamin G., Acting United States Attorney

Gyires, Marton, Assistant United States Attorney

Hernandez, Christine, Assistant United States Attorney

Hopkins, Hon, James M., United States Magistrate Judge

Marks, Neison, Assistant Federal Public Defender

Matthewman, Hon. William, United States Magistrate Judge

Maynard, Hon. Shaniek M., United States Magistrate Judge

Middlebrooks, Hon. Donald M., United States District Judge

Militello, Kristy, Assistant Federal Public Defender

Minor Victim 1

Minor Victim 2

Minor Victim 3

Peacock, R. Fletcher, Assistant Federal Public Defender

Rubio, Lisa Tobin, Assistant United States Attorney

Smachetti, Emily M., Assistant United States Attorney

Trader, Scott Joseph, Defendant/Appellant

United States of America, Plaintiff/Appellee

Villafana, Marie, Assistant United States Attorney

s/Fletcher Peacock
Fletcher Peacock, AFPD

STATEMENT OF COUNSEL

I express a belief, based on a reasoned and studied professional judgment, that this appeal involves the following questions of exceptional importance:

Issue: Whether the panel was correct in holding that the government's warrantless procurement of 31 days of continuous IP address monitoring by the cell phone application Kik was not location monitoring, and therefore, did not fall within the *Carpenter* exception to the third party doctrine.

I express a belief, based on a reasoned and studied professional judgment, that the panel decision is contrary to the following decision of the Supreme Court of the United States and that consideration by the full Court is necessary to secure and maintain uniformity of decisions in this Court:

Carpenter v. United States, ___ U.S. ___, 138 S.Ct. 2206 (2018)

s/Fletcher Peacock
Fletcher Peacock
Attorney for Appellant

TABLE OF CONTENTS

TABLE OF CITATIONS

CASES:

STATUTORY AND OTHER AUTHORITY:

STATEMENT OF THE ISSUE MERITING *EN BANC* REVIEW

ISSUE

Whether the panel was correct in holding that the government's warrantless procurement of 31 days of continuous IP address monitoring by the cell phone application Kik was not location monitoring, and therefore, did not fall within the *Carpenter* exception to the third party doctrine.

COURSE OF PROCEEDINGS AND DISPOSITION OF THE CASE

Statement of the Case

On June 13, 2017, Mr. Trader was charged by indictment with: **Count 1**, enticing a minor to engage in sexual activity, in violation of 18 U.S.C. § 2422(b); **Count 2**, distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); **Count 3**, possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2); and **Counts 4 and 5**, enticement of a minor to produce a sexually explicit video, in violation of 18 U.S.C. § 2251(a) and (e). (DE 7).

On September 6, 2017, Mr. Trader filed a motion to suppress illegally obtained evidence. (DE 13). The government responded. (DE

14). On September 25, 2017, the district court denied the motion and entered a written order. (DE 15).

Mr. Trader entered a conditional plea of guilty to Counts 1 – 5 on September 29, 2017, expressly reserving his right to appeal the district court's denial of his suppression motion. (DE 18). The United States Probation Office concluded that Mr. Trader's Sentencing Guideline range was life imprisonment, based upon an offense level of 43 and a criminal history category of III. Presentence Investigation Report (PSR). Mr. Trader filed a motion requesting a downward variance. (DE 34).

On December 7, 2017, the district court sentenced Mr. Trader to life imprisonment and a life time term of supervised release. (DE 37). Mr. Trader filed a timely notice of appeal on December 18, 2017. (DE 44).

The Appeal

Mr. Trader appealed the district court's denial of his suppression motion to this Court. The case was briefed and set for oral argument.

In his initial brief Mr. Trader argued that "the government unreasonably invaded Mr. Trader's privacy by requesting records of his location and other Internet account information from Kik and Comcast under 18 U.S.C. § 2702(b) and (c)." Appellant's Initial Brief, at 14. He

expressly relied on the Supreme Court precedent of *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038 (2001) and *Carpenter v. United States*, ___ U.S. ___, 138 S.Ct. 2206 (2018). Mr. Trader urged that the government's § 2702 request enabled the agents to monitor his location throughout the 30-day request period, and further, the case agent "relied on this location information in his search warrant affidavit to establish that Mr. Trader resided at the searched residence." Appellant's Initial brief, at 17. Mr. Trader went on to argue that the information obtained was more invasive than that obtained in *Carpenter* because it was "primarily information obtained from *within the defendant's home*." *Id.*, at 17–18 (emphasis in original). Quoting *Payton v. New York*, the argument continued:

> [A] greater burden is placed . . . on officials who enter a home or dwelling without consent. Freedom from intrusion into the home or dwelling is the archetype of the privacy protection secured by the Fourth Amendment.'" *Payton v. New York*, 445 U.S. 573, 586, 100 S.Ct. 1371, 1380 (1980) (quoting *Dorman v. United States*, [485 F.2d 385 (D.C. Cir. 1970)]). By monitoring when Mr. Trader signed onto KiK through the modem in his home, law enforcement was conducting its search within the confines of his home without a warrant. Such a search is more intrusive than CSLI gathered from public locations.

Appellant's Initial Brief, at 18. The argument regarding *Carpenter* and heightened scrutiny of intrusions into the home took five pages of the initial brief. *Id.*, at 14–18.

The government responded by arguing that *Carpenter* did not apply to this case because, "Trader had no reasonable expectation of privacy in the Kik records provided to HSI." Government Response Brief, at 24. The government reasoned that since the Kik information contained no speech content and was not continuous in nature, it did not fall within the *Carpenter* exception to the third-party doctrine.

In response, the defendant filed a reply brief that rebutted the government's argument and elaborated on the application of *Carpenter*. As part of his reply, the defendant again reemphasized the need for heightened scrutiny and cited *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Karo*, 468 U.S. 705 (1984); *Kyllo v. United States*, 533 U.S. 27 (2001) (again).

The Panel Opinion

The Court resolved Mr. Trader's appeal in a published opinion issued on November 25, 2020. *See United States v. Scott Trader*, 981 F.3d 961 (11th Cir. 2020).

In relevant part, the Court held that the Kik subscriber information for a 30-day period was not within *Carpenter's* "narrow" exception to the third party doctrine. The panel equated the Kik data to "ordinary business records like email addresses and internet protocol addresses." 981 F.3d at 968. It concluded that *Carpenter* did not consider such information, and because it did not, the information was therefore not protected. "Indisputably, email addresses and internet protocol addresses were not at issue in *Carpenter*. The third party doctrine applies..." *Id.*

The panel then took issue with the defendant's contention that the Kik records constituted "cell phone location records," as considered in *Carpenter*. "[The defendant's argument] fails on its own terms because email addresses and internet protocol addresses are neither location records nor cell phone records." *Id.* To support this conclusion, according to the panel, internet addresses do not "directly" reveal an individual's location, rather they are "a string of characters associated in an internet provider's business records with a particular device connecting the internet through a particular network." *Id.* Additionally, internet addresses can only reveal location information "indirectly, by examining

the internet company's business records to determine the physical address where the network is registered." *Id.* They are simply business records which might "incidentally" reveal location.

The panel then noted that, not just cell phones, but numerous types of devices can access the internet and therefore have internet protocol addresses. And because so many types of devices use an internet protocol address, those internet protocol addresses cannot constitute cell phone records.

Finally, the panel noted that it was not considering the defendant's "arguments Trader raises for the first time in his reply brief based on *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945 (2012); *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296 (1984); *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038 (2001)." The panel relied upon *Jones v. Sec'y. Dep't. of Corrs*, 607 F.3d 1346, 1353–54 (11th Cir. 2010).

Reasons for Granting *En Banc* Review

The panel was simply incorrect in two critical aspects of the opinion. First, internet protocol addresses are location data and are relied upon as such by law enforcement day-in and day-out. Second, the defendant did not raise a new argument in his reply brief.

The panel opinion demonstrates fundamental misconceptions about the nature of internet protocol (IP) addresses. IP addresses, as commonly used by the public, relay location data. Thus the term address. They require less translation than cellular site location information, not more. In fact, they are the "go to" means used by law enforcement to locate perpetrators of internet crimes.

The panel assumed that IP addresses are simply "a string of characters associated in an internet provider's records with a particular device connecting to the internet through a particular network." 981 F.3d at 968. That statement is true, but incomplete. In practice, the IP address is a very efficient indicator of location and is commonly used by law enforcement for that exact purpose.

The function of an IP address is to provide a unique identifier to all devices accessing the internet. The IP address is assigned to a customer by an internet provider such as Comcast or AT&T.

The internet, itself, is a form of "wide area network' (WAN). *See generally, "Wide Area Network,"* Wikipedia (https://en.wikipedia.org/wiki/Wide_area_network) (last visited 2/5/21). A single device may connect to the internet, but typically in modern usage

and in the instant case, *a "local area network" (LAN) is connected to the internet through a router at* a *fixed physical location*, such as a home or business. All of the devices in the home or business communicate with the internet through the LAN router. They can do so through hard wires or through a wireless modem. *See generally, "Local Area Network,"* Wikipedia (https://en.wikipedia.org/wiki/Local_area_network) (last visited 2/5/21).

The LAN router is assigned an IP address by the internet provider. But the devices on the LAN are not. They are automatically assigned IP addresses by the router. Identifying the router IP address is very similar to identifying the location of a cell phone tower. Both the cell phone tower and the router use their own "networks" to communicate with devices (including cell phones).

In the instant case, the local area network (LAN) used a wireless modem to connect to the internet through a router. The defendant's cell phone automatically connected with the wireless network when it came into range. All of the Kik interactions from the home were done through the wireless local area network.

The reported cases on cybercrimes are replete with references to law enforcement using IP addresses to determine the physical location of evidence and/or a suspect. *See e.g., United states v. Tisthhammer*, 484 Fed. Appx. 198, 200 (9th Cir. 2012) (government offered a series of charts displaying Internet Protocol ("IP") addresses and the geographical locations which they matched); *United States v. Renigar*, 63 F.3d 990 (10th Cir. 2010) (IP address associated with residential address sufficient to establish nexus); *United States v. Rees*, 967 F.3d 761 (7th Cir. 2020) (law enforcement tracked geographic location of device's internet protocol (IP) address to defendant's apartment); *United States v. Perez*, 712 Fed. Appx. 136 (3rd Cir. 2017) (same); *United States v. Woerner*, 709 F.3d 527 (5th Cir. 2013) (same).[1] Just because IP addresses are also used to identify devices does not mean they are not also commonly used to determine location.

The panel further stated that IP addresses do not fall within the *Carpenter* exception because they "can be translated into location information only indirectly, by examining the internet company's

[1] Anecdotally, out of dozens of cybercrime cases handled in his career, the undersigned cannot remember a single case where the investigating agent did not use an IP address to determine the location of the suspect.

business records to determine the physical address where the network is registered." 981 F.3d at 968. However, the defendant fails to see the distinction between this and the CSLI considered in *Carpenter*. The whole point of *Carpenter* was consideration of location data in the custody of a third party. The defendant respectfully suggests that "translated" overstates the effort required to recover an IP address location. It requires no more than reading a record. The CSLI information in *Carpenter,* which required analysis of hundreds of cell towers over months, presumably would have required much more translation of data.[2]

The panel cited *United States v. Hood*, 920 F.3d 87 (1st Cir. 2019) to support its contention that an IP address does not relay location information and only identifies a device. But the *Hood* decision suffers from the same faulty assumption that IP addresses do not relay location and are therefore distinguishable from CSLI. That assumption has been rightly criticized.

> Any physical location derived from IP address information also requires some limited investigatory follow-up. To be sure, an IP address does not refer to a physical location itself. This

[2] In *Carpenter*, law enforcement sought 159 days of cell tower information and received 12,898 location points. 138 S.Ct. at 2212.

> fact constitutes a distinction emphasized by the Hood court's ruling that IP address information "does not itself convey any location information." 920 F.3d at 92. But that fact may be a distinction without a difference. Practically, telecommunications providers assign IP addresses to discrete physical locations, enabling the identification of that physical location using the IP address. And as Kidd points out, it is oftentimes trivially easy to deduce that physical location using other websites.

United States v. Kidd, 394 Fed. Supp. 357, 366 (S.D.N.Y. 2019).[3]

The *Carpenter* court noted that it "when considering new innovations . . .the Court must tread carefully, to ensure that we do not 'embarrass the future.'" 138 S.Ct. at 2220. (quoting *Northwest Airlines v. Minnesota*, 322 U.S. 292, 64 S.Ct. 950 (1944). By taking such a simplistic and incomplete view of the technology involved, the panel opinion threatens to do just that. This is an important decision that should be based on rock rather than sand.

Next, the Panel's failure to address the defendant's arguments in regard to a heightened expectation of privacy in the home is not supported by the record. "And we do not consider the arguments Trader

---

[3] Additionally, *Hood* is factually dissimilar to *Carpenter* and the instant case. Law enforcement used only four days of IP address monitoring in *Hood*. In *Carpenter* it was 159 and in this case 31. It is logical that the fewer days monitored, the less likely the request will result in a comprehensive monitoring of a person's movements.

raises for the first time in his reply brief based on *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012); *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984); and *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). *See Jones v. Sec'y, Dep't of Corrs.*, 607 F.3d 1346, 1353–54 (11th Cir. 2010)." 861 F.3d at 969.

In his initial brief, the defendant clearly and completely argued that the Court should apply heightened scrutiny to the instant surveillance because the majority of it was while the defendant was in his home.

> The type of information released in the instant case is arguably even more invasive and deserving of privacy protection than the CSLI obtained in *Carpenter*. First, the KiK response was primarily information obtained from *within the defendant's home*. It is 'a basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable. . . '[A] greater burden is placed . . . on officials who enter a home or dwelling without consent. Freedom from intrusion into the home or dwelling is the archetype of the privacy protection secured by the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 586, 100 S.Ct. 1371, 1380 (1980) (quoting *Dorman v. United States*, 435 F.2d 385 (D.C. Cir. 1970)). By monitoring when Mr. Trader signed onto KiK through the modem in his home, law enforcement was conducting its search within the confines of his home without a warrant. Such a search is more intrusive than CSLI gathered from public locations.

Appellant's Initial Brief, at 17-18 (emphasis in original). Additionally, the defendant cited *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038 (2001). Appellant's Initial Brief, at 14.

Moreover, defendant's argument about heightened scrutiny was part of the larger *Carpenter* issue, also clearly raised by defendant and responded to by the government. The majority in *Carpenter* specifically discussed and relied heavily upon *Kyllo* (138 S.Ct. at 2214, 2218-19) and *Jones* (138 S.Ct. 2213, 2217, 2220) to support its holding. In light of the government's response that *Carpenter* does not apply, the defendant's discussion of *Jones*, *Kyllo* and *Karo* was both proper and necessary. It did not raise a new issue.

Finally, the panel's citation to *Jones v. Sec'y, Dep't of Corrs.*, 607 F.3d 1346, 1353–54 (11th Cir. 2010) is inapposite. In *Jones*, the appellant provided no "facts, legal arguments, or citations of authority that explain why he is entitled to a certificate on those other grounds." 607 F.3d at 1353. Jones' motion for certificate of appealability contained nothing more than two summary citations of Supreme Court precedent, and conclusory statements like, 'Certainly, reasonable jurists might differ on this issue.'" *Id.*

That is a far cry from what was argued in appellant's initial brief in this case. The defendant made his heightened scrutiny argument within the confines of a clear and thorough *Carpenter* argument. The gist of the argument was purposely placed in italics to alert the reader to the exact nature of the argument. There was a direct quote from the seminal Supreme Court case on privacy in the home *Payton v. New York*, 445 U.S. 573, 586, 100 S.Ct. 1371, 1380 (1980) and why greater scrutiny is required of such searches.

This is a difficult, but important, issue. The parties have worked long and hard on this case. If the Court, after considering the heightened scrutiny argument, finds that it is not applicable or valid, so be it. But the opinion should not rest, to any degree, upon an unwarranted waiver.

Finally, the defendant respectfully suggests that this case would have benefited greatly from an evidentiary hearing. The defendant requested one but the lower court denied that request. An evidentiary hearing would permit the parties to develop both the particular facts of the case and the extremely important technological aspects of Kik and its relation to IP addresses. A remand for such an evidentiary hearing would be appropriate.

APPENDIX

CONCLUSION

WHEREFORE the defendant requests that the Court rehear this case *en banc*.

MICHAEL CARUSO
FEDERAL PUBLIC DEFENDER

s/Fletcher Peacock
Fletcher Peacock
Assistant Federal Public Defender
109 North 2nd Street
Fort Pierce, Florida 34950
Telephone No. (772) 489-2123
Email: fletcher_peacock@fd.org

CERTIFICATE OF COMPLIANCE

I CERTIFY that this petition complies with the type-volume limitation and typeface requirements of Fed. R. App. P. 32(a)(7)(B), because it contains 2,888 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

This petition also complies with the requirements of Fed. R. App. P. 32(a)(5) and (a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14 point, Century Schoolbook font.

s/Fletcher Peacock
Fletcher Peacock

CERTIFICATE OF SERVICE

I HEREBY certify that on this 10th day of February, 2021, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and sent 15 copies to the Clerk of the Court via third party commercial carrier for delivery within three days. I also certify that the foregoing document is being served this day via CM/ECF on Christine Hernandez, Assistant United States Attorney, 99 N.E. 4th Street, Miami, Florida 33132 and Emily M. Smachetti, Chief, Appellate Division, United States Attorney's Office, 99 N.E. 4th Street, Miami, Florida 33132.

s/Fletcher Peacock
Fletcher Peacock

A-47

UNITED STATES DISTRICT COURT

Southern District of Florida
Fort Pierce Division

UNITED STATES OF AMERICA
v.
SCOTT JOSEPH TRADER

JUDGMENT IN A CRIMINAL CASE

Case Number: **17-14047-CR-MIDDLEBROOKS**
USM Number: **16118-104**

Counsel For Defendant: **Fletcher Peacock**
Counsel For The United States: **Marton Gyires**
Court Reporter: **Diane Miller**

The defendant pleaded guilty to count(s) One through Five.

The defendant is adjudicated guilty of these offenses:

TITLE & SECTION	NATURE OF OFFENSE	OFFENSE ENDED	COUNT
18 U.S.C. §2422(b)	Enticement of a minor to engage in sexual activity	05/31/2017	1
18 U.S.C. §2252(a)(2),(b)(1)	Distribution of material containing visual depictions of sexual exploitation of minors	05/30/2017	2
18 U.S.C. §2252(a)(4)(B),(b)(2)	Possession of matter containing visual depictions of sexual exploitation of minors	06/01/2017	3
18 U.S.C. §2251(a),(e)	Production of material containing visual depictions of sexual exploitation of minors	05/31/2017	4
18 U.S.C. §2251(a),(e)	Production of material containing visual depictions of sexual exploitation of minors	11/28/2015	5

The defendant is sentenced as provided in the following pages of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

Date of Imposition of Sentence: **12/7/2017**

Donald M. Middlebrooks
United States District Judge

Date: 12/8/17

DEFENDANT: **SCOTT JOSEPH TRADER**
CASE NUMBER: **17-14047-CR-MIDDLEBROOKS**

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of **LIFE. This term consists of Life as to Count One, 240 Months as to each of Counts Two and Three and 360 Months as to each of Counts Four and Five, all to be served concurrently.**

The court makes the following recommendations to the Bureau of Prisons:

1. **The Defendant participate in the Sex Offender Management Program located in the BOP at Marianna, Florida.**
2. **The Defendant be designated to a facility in or as close to Northern Florida (Marianna) as possible.**

The defendant is remanded to the custody of the United States Marshal.

RETURN

I have executed this judgment as follows:

_____

_____

_____

_____

_____

_____

Defendant delivered on _____ to _____

at _____, with a certified copy of this judgment.

_____
UNITED STATES MARSHAL

_____
DEPUTY UNITED STATES MARSHAL

DEFENDANT: **SCOTT JOSEPH TRADER**
CASE NUMBER: **17-14047-CR-MIDDLEBROOKS**

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be on supervised release for a term of **LIFE. This term consists of Life as to each of Counts One through Five, to run concurrently.**

The defendant must report to the probation office in the district to which the defendant is released within 72 hours of release from the custody of the Bureau of Prisons.

The defendant shall not commit another federal, state or local crime.

The defendant shall not unlawfully possess a controlled substance. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

The defendant shall not possess a firearm, ammunition, destructive device, or any other dangerous weapon.

The defendant shall cooperate in the collection of DNA as directed by the probation officer.

If this judgment imposes a fine or restitution, it is a condition of supervised release that the defendant pay in accordance with the Schedule of Payments sheet of this judgment.

The defendant must comply with the standard conditions that have been adopted by this court as well as with any additional conditions on the attached page.

STANDARD CONDITIONS OF SUPERVISION

1. The defendant shall not leave the judicial district without the permission of the court or probation officer;
2. The defendant shall report to the probation officer and shall submit a truthful and complete written report within the first fifteen days of each month;
3. The defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;
4. The defendant shall support his or her dependents and meet other family responsibilities;
5. The defendant shall work regularly at a lawful occupation, unless excused by the probation officer for schooling, training, or other acceptable reasons;
6. The defendant shall notify the probation officer at least ten days prior to any change in residence or employment;
7. The defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any controlled substance or any paraphernalia related to any controlled substances, except as prescribed by a physician;
8. The defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered;
9. The defendant shall not associate with any persons engaged in criminal activity and shall not associate with any person convicted of a felony, unless granted permission to do so by the probation officer;
10. The defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view of the probation officer;
11. The defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer;
12. The defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court; and
13. As directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

DEFENDANT: **SCOTT JOSEPH TRADER**
CASE NUMBER: **17-14047-CR-MIDDLEBROOKS**

SPECIAL CONDITIONS OF SUPERVISION

Adam Walsh Act Search Condition - The defendant shall submit to the U.S. Probation Officer conducting periodic unannounced searches of the defendant's person, property, house, residence, vehicles, papers, computer(s), other electronic communication or data storage devices or media, include retrieval and copying of all data from the computer(s) and any internal or external peripherals and effects at any time, with or without warrant by any law enforcement or probation officer with reasonable suspicion concerning unlawful conduct or a violation of a condition of probation or supervised release. The search may include the retrieval and copying of all data from the computer(s) and any internal or external peripherals to ensure compliance with other supervision conditions and/or removal of such equipment for the purpose of conducting a more thorough inspection; and to have installed on the defendant's computer(s), at the defendant's expense, any hardware or software systems to monitor the defendant's computer use.

Computer Possession Restriction - The defendant shall not possess or use any computer; except that the defendant may, with the prior approval of the Court, use a computer in connection with authorized employment.

Data Encryption Restriction - The defendant shall not possess or use any data encryption technique or program.

Employer Computer Restriction Disclosure - The defendant shall permit third party disclosure to any employer or potential employer, concerning any computer-related restrictions that are imposed upon the defendant.

Mental Health Treatment - The defendant shall participate in an approved inpatient/outpatient mental health treatment program. The defendant will contribute to the costs of services rendered (co-payment) based on ability to pay or availability of third party payment.

No Contact with Minors - The defendant shall have no personal, mail, telephone, or computer contact with children/minors under the age of 18 or with any the victim. The Court does not have any objection if the victim wanted to be in contact with the defendant but has to be at the initiation of the victim.

No Involvement in Youth Organizations - The defendant shall not be involved in any children's or youth organization.

Restricted from Possession of Sexual Materials - The defendant shall not buy, sell, exchange, possess, trade, or produce visual depictions of minors or adults engaged in sexually explicit conduct. The defendant shall not correspond or communicate in person, by mail, telephone, or computer, with individuals or companies offering to buy, sell, trade, exchange, or produce visual depictions of minors or adults engaged in sexually explicit conduct.

Sex Offender Registration - The defendant shall comply with the requirements of the Sex Offender Registration and Notification Act (42 U.S.C. § 16901, et seq.) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in which he or she resides, works, is a student, or was convicted of a qualifying offense.

Sex Offender Treatment - The defendant shall participate in a sex offender treatment program to include psychological testing and polygraph examination. Participation may include inpatient/outpatient treatment, if deemed necessary by the treatment provider. The defendant will contribute to the costs of services rendered (co-payment) based on ability to pay or availability of third party payment.

DEFENDANT: **SCOTT JOSEPH TRADER**
CASE NUMBER: **17-14047-CR-MIDDLEBROOKS**

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	Assessment	Fine	Restitution
TOTALS	$500.00	$0.00	$TBD

The determination of restitution is deferred until TBD . An Amended Judgment in a Criminal Case (AO 245C) will be entered after such determination.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

NAME OF PAYEE	TOTAL LOSS*	RESTITUTION ORDERED	PRIORITY OR PERCENTAGE
		TBD	

* Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

**Assessment due immediately unless otherwise ordered by the Court.

DEFENDANT: **SCOTT JOSEPH TRADER**
CASE NUMBER: **17-14047-CR-MIDDLEBROOKS**

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

A. Lump sum payment of $500.00 due immediately.

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

This assessment/fine/restitution is payable to the CLERK, UNITED STATES COURTS and is to be addressed to:

U.S. CLERK'S OFFICE
ATTN: FINANCIAL SECTION
400 NORTH MIAMI AVENUE, ROOM 08N09
MIAMI, FLORIDA 33128-7716

The assessment/fine/restitution is payable immediately. The U.S. Bureau of Prisons, U.S. Probation Office and the U.S. Attorney's Office are responsible for the enforcement of this order.

Defendant and Co-Defendant Names and Case Numbers (including defendant number), Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

CASE NUMBER DEFENDANT AND CO-DEFENDANT NAMES (INCLUDING DEFENDANT NUMBER)	TOTAL AMOUNT	JOINT AND SEVERAL AMOUNT

The defendant shall forfeit the defendant's interest in the following property to the United States: Defendant's right, title and interest to the property identified in the plea agreement and in the Preliminary Order of Forfeiture (D.E. 25) which has been entered by the Court on October 20, 2017 and is incorporated by reference herein, is hereby forfeited.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) penalties, and (8) costs, including cost of prosecution and court costs.