UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA	)	
v.	)	C.R. No. 16-00055 WES
JORDAN MONROE,	)	
Defendant.	)	

MEMORANDUM & ORDER

On May 12, 2016, law enforcement agents executed a search warrant for the Warwick, Rhode Island residence of Defendant Jordan Monroe. The agents' search uncovered a hoard of child pornography on various computers and digital storage devices. A federal grand jury subsequently indicted Monroe for allegedly producing, receiving, and possessing such materials in violation of 18 U.S.C. §§ 2251 and 2252.

The trail of digital breadcrumbs that led to Monroe's door began with several pornographic videos downloaded from an internet file sharing service by an unknown user. Pursuant to § 2703(d) of the Stored Communications Act, the Government obtained orders from two federal magistrate judges from the District of Columbia requiring the Georgia-based file sharing service to disclose the unique internet protocol ("IP") address for any device that had downloaded the illicit files. The Government later learned from

an internet service provider that the disclosed IP address was assigned to an individual at Monroe's residence.

Monroe has moved for an order suppressing "all evidence obtained as a result of the unlawful acquisition of [his] IP address." (Def.'s Mot. to Suppress 1, ECF No. 24.) He argues that the § 2703(d) disclosure orders were void ab initio because the District of Columbia magistrate judges lacked jurisdiction over the alleged crime. Relying on the Supreme Court's reasoning in Carpenter v. United States, 138 S. Ct. 2206 (2018), Monroe also contends that the Government violated his Fourth Amendment rights by procuring his IP address without a search warrant supported by probable cause. Neither argument is tenable. Thus, for the reasons stated below, Monroe's Motion to Suppress (ECF No. 24) is DENIED.

I. Background

In September 2015, agents from Homeland Security Investigations ("HSI") and personnel from the U.S. Department of Justice's Child Exploitation and Obscenity Section, High Technology Investigative Unit ("CEOS-HTIU") jointly investigated an internet-based bulletin board dedicated to the advertisement, distribution, and production of child pornography.[1] (Search Warrant Appl. Aff. of

[1] The events leading up to the May 12, 2016 search are not disputed. (See Def.'s Further Mem. in Support of Mot. to Suppress ("Def.'s Supp. Mem.") 3, ECF No. 36.)

James V. Richardson ("Richardson Aff.") ¶¶ 6, 10, ECF No. 25-5.) The bulletin board is located on "The Onion Router" or "TOR," a network which masks users' location and usage data to avoid surveillance. (Id. ¶ 7.) Only members can download content from the bulletin board; a prospective member must post pornographic content to the site to access additional privileges. (Id. ¶ 8.)

Investigators identified and captured content from numerous board posts throughout the autumn and early winter. (Id. ¶ 10.) These posts included links to URLs[2] enabling members to view and download video files. (See 1/4/16 Appl. for § 2703(d) Order ("1/4/16 Appl.") ¶¶ 5-6, ECF No. 25-3; 12/7/15 Appl. for § 2703(d) Order ("12/7/15 Appl.") ¶¶ 5-6, ECF No. 25-1.) HSI agents working at the CEOS-HTIU in Washington, D.C. accessed the bulletin board in an undercover capacity, downloaded the suspect video files from the posts' URLs, and reviewed the files to confirm their illicit content. (Richardson Aff. ¶¶ 10-11; 12/7/15 Appl. ¶ 6.)

The video files posted to the bulletin board were stored or "hosted" on servers maintained by a separate, cloud-based file sharing site ("FSS"). (See Richardson Aff. ¶ 12.) In the ordinary course of its business, the FSS maintains records about users who

[2] URL is an abbreviation for "universal resource locator" or "uniform resource locator," which constitutes "the unique address for a file that is accessible on the internet." (12/7/15 Appl. for § 2703(d) Order ¶ 5, ECF No. 25-1.)

upload or download content to its servers, including the IP addresses of devices associated with such events.[3] (See id. ¶ 16; 12/7/15 Appl. ¶ 7.) The FSS maintains its operations and stores its data in Atlanta, Georgia. (See 12/7/15 Appl. at 1.)

In early December, the Government applied to the United States District Court for the District of Columbia under 18 U.S.C. § 2703(d) for an order compelling the FSS to produce its records for eleven URLs linking to video files depicting child pornography. (See generally id.) A District of Columbia magistrate judge granted the application. (See Order 1, ECF No. 25-2.) The order required the FSS to disclose, among other records: (1) the IP address of any device that uploaded or downloaded content from the target URLs; and (2) the dates and times these files were uploaded or downloaded. (Id. at Attach. A.) The Government followed an identical investigative process to support an application for a § 2703(d) order for records related to eighteen more URLs on January 6, 2016. (See generally 1/4/16 Appl.) The January application was also granted. (See Order 1, ECF No. 25-4.)

The records produced in response to the orders revealed that two particular IP addresses downloaded or attempted to download the illicit content hosted by the FSS' servers on October 27, 2015

[3] As defined by the Government, an IP address is "a unique number used by a computer to access the Internet, and can be used to determine where a computer or mobile device is located." (12/7/15 App. ¶ 7.)

and December 31, 2015. (Richardson Aff. ¶¶ 17, 27.) Using publicly available search tools, the Government identified the internet service provider that controlled these IP addresses. (Id. ¶¶ 18, 28.) The internet service provider, in response to Department of Justice subpoenas, disclosed that in both instances the IP address was assigned to a subscriber at Monroe's Warwick, Rhode Island residence. (Id. ¶¶ 19, 29.) Government agents conducted further surveillance and investigated the home's occupants, including Monroe. (Id. ¶¶ 20-24.)

On May 10, 2016, the Government set forth the substance of these facts in an application for a search warrant for the Warwick residence. (See generally Appl. for Search Warrant, ECF No. 25-5.) The application was submitted to and approved by a magistrate judge for the United States District Court for the District of Rhode Island. (See Search & Seizure Warrant, ECF No. 25-5.) Agents executed the search warrant two days later, uncovering the cache of child pornography. (See Aff. of James V. Richardson in Support of an Appl. for Cr. Compl. 2-3, ECF No. 1-2). Monroe made incriminating statements to government agents during a contemporaneous interview. (Id. at 3; see also Mem. & Order 9-19, ECF No. 29 (denying motion to suppress statements made during interrogation in Monroe's home).)

II. Discussion

A. Did the District of Columbia Magistrate Judges Have Jurisdiction to Issue the § 2703(d) Orders?

The privacy of stored electronic communications and transactional records is governed by the federal Stored Communications Act ("SCA"). See generally 18 U.S.C. §§ 2701-2711. Section 2703 of the SCA specifically establishes "the rules that the government must follow when it seeks to compel a [third-party service] provider to disclose information." Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it, 72 Geo. Wash. L. Rev. 1208, 1218 (2004).[4] The standard the Government must satisfy to compel disclosure varies with the nature of the materials requested. Basic subscriber information such as a customer's name, address, or payment details may be easily procured from a provider through a subpoena. See 18 U.S.C. § 2703(c)(2). If the Government seeks the content of stored electronic communications, it must obtain a search warrant or serve a lesser form of process – an administrative subpoena or § 2703(d) order, discussed below – and provide prior notice to the subscriber or customer. See id. § 2703(a)-(b).

The Government's request for IP address information here falls into a third category: "[r]ecords concerning electronic communication service or remote computing service." Id. § 2703(c).

[4] There is no dispute that the FSS was covered by the statute.

Neither a search warrant nor prior notice are required to compel a provider to produce this information. See id. At a minimum, however, the Government must apply to a court and "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of . . . the records or other information . . . are relevant and material to an ongoing criminal investigation." Id. § 2703(d).

Any court of "competent jurisdiction" may issue a §2703(d) disclosure order. Id. The SCA defines courts of "competent jurisdiction" to include "any district court of the United States (including a magistrate judge of such a court)" with "jurisdiction over the offense being investigated." Id. § 2711(3). The district where the provider is located may also authorize disclosure. Id. § 2711(3)(ii).

The United States Constitution requires that crimes be prosecuted where the offenses were committed. See United States v. Rodriguez-Moreno, 526 U.S. 275, 278 (1999) (quoting U.S. Const. art. III, § 2, cl. 3); see also Fed. R. Crim. P. 18 ("[T]he government must prosecute an offense in a district where the offense was committed."). As the Sixth Circuit has observed, however, "federal obscenity laws, by virtue of their inherent nexus to interstate and foreign commerce, generally involve acts in more than one jurisdiction or state." United States v. Thomas, 74 F.3d 701, 709 (6th Cir. 1996). Offenses under 18 U.S.C. §§ 2251 and

2252 are thus widely recognized as "continuing offenses" often occurring in more than one district. See, e.g., United States v. Kapordelis, 569 F.3d 1291, 1308 (11th Cir. 2009); United States v. Moncini, 882 F.2d 401, 403 (9th Cir. 1989); United States v. Cameron, 733 F. Supp. 2d 177, 181 (D. Me. 2010). Under such circumstances, jurisdiction is proper in "any district from, through, or into which" obscene material moves. 18 U.S.C. § 3237(a); see also United States v. Langford, 688 F.2d 1088, 1094 (7th Cir. 1982), cert. denied 461 U.S. 959 (1983) (holding § 3237(a) "authorizes federal obscenity cases to be venued in . . . any jurisdiction through which the mailed obscene material moves"); United States v. Peraino, 645 F.2d 548, 551 (6th Cir. 1981) (same); Cameron, 733 F. Supp. 2d at 181 (same).

The forgoing principles gut Monroe's contention that the orders requiring the FSS to produce his IP address were void ab initio. Government agents downloaded the obscene videos hosted by the FSS's servers at the CEOS-HTIU in Washington, D.C. (Richardson Aff. ¶¶ 10-11.) Because some of the material involved in the offenses under investigation – the video files - moved through the District of Columbia, it was a court of "competent jurisdiction" under the SCA. See Thomas, 74 F.3d at 709; Langford, 688 F.2d at 1094; see also United States v. Bagnell, 679 F.2d 826, 830 (11th Cir. 1982), cert. denied, 460 U.S. 1047 (1983) ("[T]here is no constitutional impediment to the government's power to prosecute

pornography dealers in any district into which the material is sent."); United States v. McVicker, 979 F. Supp. 2d 1154, 1177 (D. Or. 2013) (finding federal agent's download of child pornography files within district enough to establish jurisdiction under § 3237(a)). No personal acts by a defendant within the district are required; even a government agent's conduct is sufficient to cement jurisdiction. See, e.g., United States v. Chi Tong Kuok, 671 F.3d 931, 938 (9th Cir. 2012) (affirming validity of prosecution where undercover agent's conduct occurred in the district); United States v. Angotti, 105 F.3d 539, 543 (9th Cir. 1997) (recognizing "venue will often be possible in districts with which the defendant had no personal connection, and which may occasionally be distant from where the defendant originated the actions constituting the offense"); United States v. Stokes, No. 6:12–CR–03091–MDH–1, 2014 WL 2895409, at *2 (W.D. Mo. June 26, 2014) (finding prosecution within district proper as investigating agent received obscene images on a computer within the district).[5]

The Court is not convinced by Monroe's argument that the Supreme Court's "analysis of [a district court's] territorial reach" in Dahda v. United States, 138 S. Ct. 1491, 1495 (2018),

[5] See also United States v. Luton, 486 F.2d 1021, 1022 (5th Cir. 1973), cert. denied, 417 U.S. 920 (1974) ("Both venue and territorial jurisdiction of a federal district court in criminal cases depend on some part of the criminal activity having occurred within its territory.")

supports exclusion of his IP address and any fruits derived therefrom. (See Def.'s Supp. Mem. 10) Whether a non-constitutional, statutory violation requires a court to throw out evidence turns on the particular language of the statute. United States v. Donovan, 429 U.S. 413, 432 n.22 (1977). Dadha interprets the federal wiretap statute, not the SCA. Dahda, 138 S. Ct. at 1494. And unlike the wiretap statute, the SCA does not include suppression among its exclusive remedies for violations. Compare 18 U.S.C. § 2518(10)(a)(iii) (intercepted communication must be suppressed if order is "insufficient on its face") with 18 U.S.C. §§ 2701, 2707 (providing "only judicial remedies" available for non-constitutional SCA violations are criminal prosecution and civil damages) (emphasis added); United States v. Gasperini, No. 16-CR-441 (NGG), 2017 WL 3038227, at *3 (E.D.N.Y. July 17, 2017), aff'd, 894 F.3d 482 (2d Cir. 2018) ("Statutory violations of the SCA, without more, are not remedied through exclusion of the resulting evidence in court.").

The Supreme Court's acknowledgment in Dahda that the wiretap statute expressly limits a district judge's power to authorize communication intercepts to "the territorial jurisdiction of the court in which the judge is sitting," 138 S. Ct. at 1495, is thoroughly consistent with the outcome here: the District of Columbia's jurisdiction over the alleged crime of distributing child pornography was established when the investigators downloaded the

illicit files within its boundaries. The magistrate judges did not transgress the territorial limits of their authority.

B. Does Carpenter v. United States Require the Government to Obtain a Warrant to Compel the Disclosure of IP Addresses?

Monroe also argues that this Court should apply the reasoning articulated in Carpenter v. United States, 138 S. Ct. 2206 (2018), to find that the Constitution requires the Government to obtain a warrant supported by probable cause to compel the disclosure of an IP address. (Def.'s Supp. Mem. 3-9.) The Court is unpersuaded, however, that the Government's acquisition of a defendant's historical cell site location information ("CSLI") from a third party is analogous to the circumstances here.

In Carpenter, the Supreme Court considered whether an individual maintained a legitimate expectation of privacy under the Fourth Amendment in the extensive record of his physical movements captured by wireless carriers through CSLI. See 138 S. Ct. at 2219. In answering "yes," the Court focused on the unique nature of CSLI. "A cell phone," Chief Justice Roberts wrote, is "almost a 'feature of human anatomy.'" Id. at 2218 (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)). CSLI "tracks nearly exactly the movement of [a cell phone's] owner," enabling the Government to obtain "near perfect surveillance" in both public and private locales "as if it had attached an ankle monitor to the phone's user." Id.

The FSS's record of Monroe's IP address was not an "exhaustive chronicle" of his physical or digital activities. See id. at 2219. Although an IP address is a unique numerical identifier, see United States v. Kearney, 672 F.3d 81, 84 n.1 (1st Cir. 2012), it can only provide "the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones." In re BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 84 (E.D.N.Y. 2012). It does not, in and of itself, reveal a particular user's identity or the content of the user's communications.[6] Indeed, a "subscriber to whom a certain IP address was assigned may not be the same person who used the Internet connection for illicit purposes." SBO Pictures, Inc. v. Does 1-3036, No. 11-4220 SC, 2011 WL 6002620, at *3 (N.D. Cal. Nov. 30, 2011). More investigation is required to establish such facts. This understanding is consistent with the additional steps taken by the Government to tie Monroe to the illicit video files, including determining the internet service provider that owned the IP address, subpoenaing the provider's subscriber information, and conducting additional surveillance. (Richardson Aff. ¶¶ 17-24, 28-29.)

[6] If the Government seeks to compel content, the SCA expressly requires the government to obtain a search warrant or provide a subscriber with prior notice. See 18 U.S.C. § 2703(a)-(b).

An IP address is one link held by a third party in a chain of information that may lead to a particular person. It does not reveal the kind of minutely detailed, historical portrait of "the whole of [a person's] physical movements" that concerned the Supreme Court in Carpenter, 138 S. Ct. at 2219. This information is more akin to the records of dialed numbers kept by a telephone company. See United States v. Tolbert, 326 F. Supp. 3d 1211, 1225 (D.N.M. July 27, 2018) (comparing "identifying data" in IP address to telephone and bank records and finding such data did not "rise to the level of the evidence in Carpenter"). Individuals have no reasonable expectation of privacy in such records. See Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (no protected privacy interest in telephone records of numbers dialed); United States v. Miller, 425 U.S. 435, 440-41 (1976) (no protected privacy interest in bank records). The Carpenter Court expressly declined to disturb those rulings. 138 S. Ct. at 2220. The § 2703(d) orders therefore were sufficient to compel the FSS to disclose Monroe's IP address.[7]

[7] In light of this ruling, the Court does not reach whether the good faith or inevitable discovery exceptions would otherwise defeat Monroe's request for exclusion. (See generally Gov.'s Resp. to Def.'s Supp. Mem. 12-15, ECF No. 38.)

III. Conclusion

For the foregoing reasons, Defendant Jordan Monroe's Motion to Suppress (ECF No. 24) is DENIED.

IT IS SO ORDERED.

William E. Smith
Chief Judge
Date: November 1, 2018