UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CRIMINAL ACTION NO. 19-10073-RGS

UNITED STATES OF AMERICA

v.

STEVEN CARME

MEMORANDUM AND ORDER ON DEFENDANT'S MOTION TO SUPPRESS AND MOTION FOR A *FRANKS* HEARING

June 17, 2020

STEARNS, D.J.

Defendant Steven Carme is charged in a three-count indictment with possession, receipt, and distribution of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and § 2252A(a)(5)(B) and (b)(2). He seeks now to suppress files containing images of child pornography downloaded from network postings generated by his personal computer. After a hearing on the motion, for the reasons to be stated, suppression of the images will be DENIED.

The essential facts are not in dispute. Carme subscribed to a "peer-to-peer" file-sharing software called BitTorrent. As the name implies, BitTorrent allows a subscriber to assemble a file of interest from fragments scattered over computers linked to a shared network. In return, the user is

expected to leave his assembled file open on the network for other users with similar interests to access. The declared ethos of the BitTorrent community is one of sharing, not anonymity. Thus, when joining a BitTorrent "storm," a user is expected to make his Internet Protocol (IP) address available to all the other members of his group by staying connected to the network.

This case arose during a two-year online investigation undertaken by Barnstable Police Detective Kevin Connolly of the IP address 174.62.202.4, which was suspected to offer BitTorrent users access to files containing child pornography. Using a law enforcement computer equipped with a BitTorrent-deciphering software known as Roundup Torrential Downpour, on Saturday, October 20, 2018, Connolly established a four-hour connection with the computer at the suspect IP address. He succeeded in downloading 192 public files, four of which contained entire videos and 182 of which contained partial videos. (Five files could not be opened). FBI Special Agent Bryce Montoya, who assisted the investigation, determined that at least three of the full videos depicted children engaged in explicit sexual conduct.[1]

As more fully explained by the Eighth Circuit in *United States v. Hoeffener*, 950 F.3d 1037 (8th Cir. 2020):

[1] In his affidavit in support of the search warrant at issue, Agent Montoya described the videos in detail and provided still images of child pornography he had copied from them.

> Torrential Downpour is a law enforcement software program configured to search the BitTorrent network for Internet Protocol ("IP") addresses associated with individuals offering to share or possess files known to law enforcement to contain images or videos of child pornography. Detective Robert Erdely, an investigator for the Indiana County, Pennsylvania District Attorney's Office, testified that the program logs the date, time, and infohash of the activity occurring during the investigation; the path and file name investigated; and the investigated computer's IP address, port identifier, and BitTorrent software. Detectives Baine and Erdely both testified that Torrential Downpour cannot access non-public areas or unshared portions of an investigated computer, nor can it override settings on a suspect's computer.

Id. at 1040-1041. In sum, Torrential Downpour exploits a flaw in the BitTorrent software, a "trap door" that allows a "de-choking" of a BitTorrent storm that forces the fragments to recompose as an integrated "single source" downloadable file.

On February 1, 2019, Agent Montoya obtained a search warrant from Magistrate Judge Bowler for Carme's home in Marstons Mills, Massachusetts. When officers executed the search warrant at Carme's residence on February 5, 2019, a computer in a shed on the property was turned on and running the BitTorrent software. When questioned, Carme admitted that he had used the BitTorrent software and network to collect and share child pornography over the IP address of his computer.

DISCUSSION

Carme makes two objections to the legality of the search warrant. (I will invert the order in which they are presented for purposes of logical flow). First, he claims that traditional notions of privacy are "ill-suited to the digital age," Def.'s Resp. at 7 (quoting *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., dissenting), and the deployment by law enforcement officers of advanced investigative technologies like Torrential Downpour. In its more particular context, he argues that BitTorrent, by fragmenting the contents of the files being shared, gives users an extra layer of privacy, by making it impossible for law enforcement officer with access to a peer-to-peer network to view the entirety of a file without Torrential Downpour's "ability to achieve [by forced aggregation] a single source download." Def.'s Mem. at 16.

Second, he maintains that the search warrant affidavit, submitted by Agent Montoya, misled Magistrate Judge Bowler by failing to give her a full understanding of the internal workings of BitTorrent and its interface with Torrential Downpour. More specifically, he argues that the affidavit did not disclose the "specialized nature" of Torrential Downpour or the extent to which it alters "the normal" BitTorrent protocols, nor did it "completely describe . . . what makes BitTorrent different from other peer-to-peer file sharing methods." Def.'s Mem. at 18, 20.[2] Had the Magistrate Judge been

[2] The remedy that Carme seeks is a hearing pursuant to *Franks v.*

instructed properly in the specialized nature of the software, or so Carme's argument goes, it would likely have changed her evaluation of probable cause. Def.'s Mem. at 20.[3]

The roots of Carme's first argument are found in an evolving reformulation of fundamental concepts of privacy in the light of ever-more intrusive and sophisticated technology. Before the age of the Internet and the iPhone, it was generally accepted that the knowing exposure of one's intimate private affairs to public view, whether inadvertent, unavoidable, or uninvited, defeated any claim to a reasonable expectation of privacy. *See United States v. Dionisio*, 410 U.S. 1, 14-15 (1973) (voice); *United States v. Mara*, 410 U.S. 19, 21 (1973) (handwriting); *United States v. Knotts*, 460 U.S. 276, 281-282 (1983) (movements of an automobile or container on a public

---

Delaware, 438 U.S. 154 (1978), presumably as an alternative route to suppression, should the court reject his *Carpenter*-based argument.

[3] Carme does not deny that BitTorrent is a peer-to-peer (P2P) file sharing software. He concedes (as he must) that every Circuit Court to examine the issue has concluded that users of P2P software do not have an objectively reasonable expectation of privacy in the files that they make available for public sharing. *See, e.g., United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008), and Gov't.'s Opp'n at 10-12 (collecting additional cases). Rather, Carme contends that because BitTorrent breaks files into "tiny" bits and shares them with "many people," the risk of being detected by a law enforcement officer (who does not have access to Torrential Downpour) is minimized, thereby making BitTorrent "unique" and distinguishable from "older, non-BitTorrent precedent." Def.'s Resp. at 12. As the government aptly states, Carme "essentially argues that because he did not think he would get caught, he had a reasonable expectation of privacy in files he publicly shared . . . ." Gov't.'s Opp'n at 1.

thoroughfare); *Maryland v. Macon*, 472 U.S. 463, 469 (1985) (obscene magazines displayed for sale); *Dow Chemical Co. v. United States*, 476 U.S. 227, 239 (1986) (activity in open areas of an industrial complex); *United States v. Rose*, 669 F.2d 23, 25-26 (1st Cir. 1982) (ham radio transmissions).

It was also generally understood, that if the object or activity was exposed to the public, the fact that law enforcement officers used sophisticated means of detection added little to the equation. *See California v. Ciraolo*, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares"). Nor was there thought to be anything improper in the use of conventional optical aids or other devices that augment the ability of the senses to detect what is exposed to public view or perception. *Knotts*, 460 U.S. at 284 ("We have never equated police efficiency with unconstitutionality and decline to do so now."); *see also United States v. Lace*, 669 F.2d 46, 51 (2d Cir. 1982) (outdoor surveillance with a night vision device); *Dow Chemical Co.*, 476 U.S. at 229 (aerial surveillance photography of an industrial complex); *Ciraolo*, 476 U.S 213-214 (fixed-wing surveillance of a home from navigable airspace); *Florida v. Riley*, 488 U.S. 445, 451

(1989) (helicopter surveillance); *Illinois v. Caballes*, 543 U.S. 405, 409 (2005) (drug-sniffing dog).

The first hint of a shift in thinking regarding the balance between technology and privacy came in *Kyllo v. United States*, 533 U.S. 27 (2001), a case in which officers used a thermal imaging device to detect unusual heat pockets in a home suggestive of a marijuana-growing operation. The Court rejected an "off-the-wall" and "through-the-wall" detection distinction urged by the Government that "would leave the homeowner at the mercy of advancing technology," *id*. at 35, and held that the warrantless use of sophisticated sense-enhancing technology, "not in general public use," and capable of revealing private information about lawful (as well as unlawful) activities in the interior of a home "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a [presumptively unreasonable] search." *Id*. at 34; s*ee also Florida v. Jardines*, 569 U.S. 1, 11 (2013) (drug-sniffing dog inserted into the curtilage of the home – "[W]hen the government uses a physical intrusion to explore details of the home (including its curtilage), the antiquity of the tools that they bring along is irrelevant").

> High-powered telescopes, parabolic sound gathering devices, and infrared cameras are all able to gather ordinarily

> imperceptible information (in the form of light rays, sound waves, or heat waves) from the *interior* of an enclosed space as it emanates from that space. Although such devices can operate from an external and public place, their use is invasive nevertheless, because they provide information *from* an enclosed space about the enclosure's contents that a police officer, standing at a lawful vantage point, cannot detect with ordinary human powers of perception.

State v. Smith, 963 P.2d 642, 647 (Or. 1998) (emphasis in original); *see also United States v. Karo,* 468 U.S. 705, 714-715 (1984) (agents used a signaling device hidden in a can of ether to monitor movements inside defendant's home – information "that could not have been visually verified"); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251-252 (5th Cir. 1987) (continuous silent videotape surveillance of an enclosed private area must be judicially authorized).

However, with but two albeit important exceptions, the law restricting warrantless surveillance by the use of sophisticated technology has been limited to direct (and indirect) intrusions into the privacy of the home. The first of the two exceptions involves physical trespass onto private property or the person. *See United States v. Jones*, 565 U.S. 400, 416 & n.3 (2012) (the warrantless installation of a GPS tracking device on the undercarriage of defendant's vehicle amounted to an unconstitutional physical trespass on a constitutionally protected area – "for most of our history the Fourth

Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates"); *Grady v. North Carolina*, 575 U.S. 306, 309 (2015) (*per curiam*) (affixing a GPS device to a convicted sex offender – "[I]t follows [from our constitutional trespass cases] that a State also conducts a search when it attaches a device to a person's body, without consent, for the purpose of tracking that individual's movements.").

The second exception involves the "smart" phone. *See Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Riley* held that the owner of a cell phone has a reasonable expectation of privacy in digital data stored on the hard drive of the phone even where the data, or large portions of it, are cloud stored. In *Carpenter*, a 5-4 decision authored by Chief Justice Roberts, the Court went a step further, holding that the third-party records doctrine did not relieve the government of the necessity of obtaining a warrant based on probable cause to secure the production of historical cell site location information (CSLI), at least covering any extended period of time. Expressing skepticism whether the logic of the "third-party principle" as applied to telephone numbers and bank records could be stretched to cover "the qualitatively different category

of cell-site records," *id*. at 2216-2217, Chief Justice Roberts observed that "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever the owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id*. at 2217. With this in mind, he "decline[d] to extend *Smith* and *Miller* to the collection of CSLI." *Id*. at 2220.

What is important for present purposes is that Chief Justice Roberts immediately stressed that the decision was a "narrow one," and should not be read "to disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras." *Id*. By way of further explanation: In many areas of human interaction, privacy claims are deemed *per se* unreasonable. There can be, for example (outside of the cell phone carrier, cloud-storage exception) no reasonable expectation of privacy in most matters voluntarily disclosed or entrusted to third parties. "It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs, the Fourth Amendment does not prohibit the governmental use of the now-nonprivate information." *United States v. Jacobsen*, 466 U.S. 109, 117 (1984). *See*

United States v. Miller, 425 U.S. 435, 442-443 (1976) (bank account records); *Smith v. Maryland*, 442 U.S. 735, 744-745 (1979) (numbers dialed from a subscriber's telephone); *United States v. Forrester*, 512 F.3d 500, 509-510 (9th Cir. 2008) (addresses of outgoing emails); *United States v. Meriwether*, 917 F.2d 955, 959 (6th Cir. 1990) (numbers transmitted to a third party's pager); *State v. Marcum*, 319 P.3d 681, 687 (Okla. Crim. App. 2014) (text messages sent to a third-party's cell phone); *United States v. Payner*, 447 U.S. 727, 731-732 (1980) (records entrusted to a bank officer); *cf. United States v. Wahchumwah*, 704 F.3d 606, 610-611 (9th Cir. 2012) (audio-video recording of an illegal transaction by an invitee into defendant's home).

At bottom, what Carme is urging is an extension of *Carpenter*'s expanded privacy protections to include software enabling the sharing of child pornography through a technology more difficult to detect than traditional P2P file sharing. As no one person could plausibly keep track of the entirety of a person's movements over time as reflected in compiled CSLI data, Carme argues that because no one could see an entire file on his BitTorrent site, but only "a small piece of the file," this court should "recognize that the aggregation of information might be covered by a

reasonable expectation of privacy, even though each particular discrete set of data on its own would not." Def.'s Resp. at 13.

To embrace Carme's argument would require this court to essentially overrule the third-party exposure doctrine and the array of circuit cases holding (consistent with longstanding Supreme Court precedent), that "[a]n individual does not have an expectation of privacy in items or places he exposes to the public." *United States v. Bucci*, 582 F.3d 108, 117 (1st Cir. 2009). More specifically, this court would be required to overrule (or substantially mangle) *United States v. Morel*, 922 F.3d 1 (1st Cir. 2019), in which the identical "*Carpenter* . . . effected a sea change" argument was raised and rejected. *Id*. at 8. As the First Circuit noted in *Morel*, "*Carpenter* did not announce a wholesale abandonment of the third-party doctrine." *Id*. at 8; see *also United States v. Hood*, 920 F.3d 87, 91 (1st Cir. 2019) (a computer user has no reasonable expectation of privacy in his IP address). Rewriting circuit law is simply beyond the power or the competence of this court. *See United States v. Moore-Bush*, 2020 WL 3249060 at *1 (1st Cir. June 16, 2020) ("The argument made in support of the district court's suppression order [of evidence gathered from pole camera surveillance] is that the logic of the opinion in *Carpenter* should be extended

to other technologies and other Fourth Amendment doctrines, and that this extension provides a basis to overturn this circuit's earlier precedent . . . . Nothing in *Carpenter*'s stated 'narrow' analysis triggers [an exception] to the law of the circuit doctrine.").

This disposes of Carme's *Franks* motion as well. The only potential gain for Carme from a more elaborate presentation of BitTorrent and Torrential Downpour technology to the Magistrate Judge would have been to persuade her to adopt the same erroneous *Carpenter*-based argument that this court has rejected. Consequently, an after-the-fact *Franks* hearing would accomplish nothing of value.[4]

ORDER

For the foregoing reasons, the motion to suppress is DENIED. The motion for a *Franks* hearing is also DENIED.

SO ORDERED.

/s/ Richard G. Stearns
UNITED STATES DISTRICT JUDGE

[4] I have read the affidavit and, even assuming that the Magistrate Judge was unfamiliar with computer technology (which emphatically is not the case), I find Agent Montoya's explanation of BitTorrent more than satisfactory even for one untutored in the subject.