UNITED STATES DISTRICT COURT DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA

v.

No. 3:14-cr-00185 (JAM)

CHRISTOPHER CHAVEZ, Defendant.

ORDER DENYING MOTION TO SUPPRESS

Defendant Christopher Chavez moves to suppress information acquired by the Government from his telephone company—Verizon—concerning the location of cell phone towers that were used or accessed in connection with communications involving a specific telephone number that the Government associates with defendant. Defendant principally contends that this information—known as "cell site location information"—should be suppressed because the Government did not obtain it by means of a search warrant on the basis of a showing of probable cause. Because I conclude that the Government's acquisition of this information was neither a "search" nor "seizure" that is subject to the requirements of the Fourth Amendment and because I conclude that any legal violation here would not warrant a remedy of suppression of evidence, I will deny the motion to suppress.

BACKGROUND

In June 2015, the Government applied for and obtained an order from a United States Magistrate Judge to direct Verizon to disclose records reflecting the location of cell towers relating to the use of certain cellular telephones, including a cellular telephone that was allegedly used by defendant Christopher Chavez. The Stored Communications Act is a federal law that authorizes the Government to seek such information from telecommunications companies provided that the Government first obtains a court order on the basis of an application that

identifies "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The Government's application here described the extensive background of its criminal narcotics investigation and why it would be of particular significance to identify the physical whereabouts of defendant at the time that his telephone was used from August 9 to August 31, 2014. At the oral argument of this matter, the Government stated its intention to introduce evidence at trial of a single day of defendant's cell site location information. It is apparent from my review of the Government's application that it sets forth specific and articulable facts and that the requested cell-site location information was clearly relevant and material to the Government's investigation of extensive cocaine trafficking operations.

DISCUSSION

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. A predicate to any claim of a Fourth Amendment violation is that there has been either a "search" or a "seizure." A "search" for purposes of the Fourth Amendment occurs when the police intrude upon a person's reasonable expectation of privacy, or if the police otherwise trespass upon a person's body, house, papers, or effects for the purpose of acquiring information. *See Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013); *United States v. Jones*, 132 S. Ct. 945, 951 n.5 (2012). A "seizure" of property for purposes of the Fourth Amendment occurs when the police meaningfully interfere with an individual's possessory interest in that property. *See Soldal v. Cook County, Ill.*, 506 U.S. 56, 61 (1992).

Here, the Government acquired information about defendant that was in the possession of a third-party—Verizon—and that the acquisition of this information did not involve any trespass upon defendant's body, house, papers, or effects and did not involve any interference at all with defendant's possessory interests in any of his property. In *United States v. Miller*, 425 U.S. 435, 440–43 (1976), the Supreme Court held that a bank customer has neither a property interest nor a reasonable expectation of privacy in banking records obtained by law enforcement from a customer's bank. A bank's records are not a customer's "private papers," but are "the business records of the banks," and a bank customer "can assert neither ownership nor possession" over such documents for Fourth Amendment purposes. *Id.* at 440. The Court further ruled that a bank customer has no reasonable expectation of privacy in his banking records, because they "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442. As the Court explained, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government," and "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443.

In essence, the Supreme Court made clear in *Miller* the basis for the so-called "third-party doctrine" of the Fourth Amendment: that a person does not have a right or interest that is protected under the Fourth Amendment to prevent the Government from obtaining information about a person that is in the custody of a third party and including information that the person has voluntarily disclosed to a third party. *See also Smith v. Maryland*, 442 U.S. 735 (1979) (customer

has no legitimate expectation of privacy in telephone company's records of telephone numbers dialed by the customer).

The third-party doctrine has been subject to tsunamis of criticism. ¹ But it doubtlessly remains good law today. *See, e.g., Am. Civ. Liberties Union v. Clapper*, 785 F.3d 787, 822 (2d Cir. 2015). The Second Circuit has yet to address whether the Fourth Amendment applies to the acquisition of cell-site location information, but it is no surprise in light of *Miller* and *Smith* that other federal appellate courts have concluded that the Fourth Amendment's warrant and probable cause requirements do not apply when the Government acquires cell-site location information from a telecommunications provider. *See United States v. Davis*, 785 F.3d 498, 506-17 (11th Cir. 2015) (en banc); *In re United States for Historical Cell Site Data*, 724 F.3d 600, 611-13 (5th Cir. 2013); *In re Application of U.S. for an Order Directing a Provider of Elec. Comme'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 313 (3d Cir. 2010); *see also In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c)*, 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless, 42 F. Supp. 3d 511, 517 (S.D.N.Y. 2014) (collecting more cases).²

Defendant has not advanced a convincing reason to distinguish the Supreme Court's rulings in *Miller* and *Smith*—that is, to show why the Government's obtaining of cell-site location information from a telephone company is materially different or more intrusive than the

¹ "The third-party doctrine is the Fourth Amendment rule scholars love to hate" and has been condemned as no less than "the *Lochner* of search and seizure law, widely criticized as profoundly misguided." Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009). *See also* Jane Bambauer, *Other People's Papers*, 94 Tex. L. Rev. 205, 262 (2015) ("the third-party doctrine has become the Fourth Amendment's supervillain" and "it puts no constitutional limits on dragnet data collection"); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975 (2007) (noting criticism of the third-party doctrine and describing alternative approaches adopted by some states for privacy protection).

A divided panel of the Fourth Circuit ruled to the contrary, but the panel's opinion has been withdrawn with the granting of the Government's petition for rehearing en banc. *See United States v. Graham*, 796 F.3d 332, 344-45 (4th Cir.), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

Government's obtaining of financial records from a customer's bank (*Miller*) or telephone dialing and toll records from a telephone company (*Smith*). Indeed, as the Government noted at oral argument, the cell-site location information—unlike a GPS tracking device—does not actually "pinpoint" the location of a telephone's user. It does no more than identify that the telephone at issue—while in use—is within certain range in a proximate direction (within a 120-degree "wedge" direction) from a specific cellular telephone tower.³

Disclosure of such broad, zonal locational information is not more intrusive than disclosure of the kind of information that is routinely disclosed in banking or credit card records concerning whom one is paying for particular products or services (*e.g.*, to pay doctors, to buy medicines, to withdraw cash from an ATM at a casino, to buy racy or artsy films, or to make religious donations, etc.). And it is not more intrusive than disclosure of the telephone numbers that someone has called (*e.g.*, telephone calls to doctors, to one's paramour, or to houses of worship, etc.). As *Miller* and *Smith* make clear, the Government's acquisition from third parties of such financial and telephone records—no matter how directly or inferentially revealing—does not intrude upon a reasonable expectation of privacy under the Fourth Amendment.

Does it matter that cell-site location information may potentially disclose that a customer is not in a public location but is in the protected sanctity of his home? Ordinarily, of course, the Fourth Amendment applies with maximum effect to what we seek to keep private in the home. And so the Fourth Amendment applies if a law enforcement agent positions himself outside someone's home and uses high-tech thermal imaging technology to try to determine details about heat patterns that are within the home. *See Kyllo v. United States*, 533 U.S. 27 (2001). Similarly, the Fourth Amendment applies if law enforcement officers place an electronic "beeper" or "bug"

³ Accordingly, the record here does not support conclusions undertaken by another district court that cell-site location information is akin to GPS tracking. *See In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 2015 WL 4594558 at *9 (N.D. Cal. 2015).

on an article of property possessed by a suspect and then use its signals to monitor the suspect within his home. *See United States v. Karo*, 468 U.S. 705 (1984).

But neither *Kyllo* nor *Karo* involved the third-party doctrine—in which a suspect voluntarily discloses information to a third party and when the Government in turn obtains such information from and with the aid of this third party. In the third-party doctrine context, it is irrelevant that a suspect has voluntarily disclosed information while in the privacy of his home and despite the fact that such disclosure doubtlessly reveals something about what a suspect has chosen to say or to do within his home. *See Smith*, 442 U.S. at 737 (no Fourth Amendment protection as to "the numbers dialed from the telephone *at petitioner's home*") (emphasis added); *United States v. White*, 401 U.S. 745 (1971) (no Fourth Amendment protection as to suspect's statements within his own home to a third-party informant who was wearing a secret radio transmission device subject to contemporaneous monitoring by law enforcement agents outside).

Defendant also contends that cell-site location information is not voluntarily conveyed to one's cellular telephone company in the same sense or manner that one voluntarily conveys financial information to a bank as in *Miller* or telephone numbers to a telephone company as in *Smith*. Although this rationale has convinced some courts to conclude that the third-party doctrine does not apply,⁴ I do not agree. Every cell phone customer knows that his or her information is relayed wirelessly to nearby cell phone towers. It can come as no surprise that one's cell phone company keeps records of cell towers that are accessed by and necessary to the provision and connection of every customer's cell phone service. This is no different than every customer's awareness that the bank keeps records of one's checks and transactions (*Miller*) and that the telephone company keeps records of the telephone numbers that one calls (*Smith*).

⁴ See, e.g., In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 2015 WL 4594558 at *12-*14 (N.D. Cal. 2015); Com. v. Augustine, 467 Mass. 230, 249-51 (2014).

Of course, no customer desires his bank or telephone company to disclose his account information to the Government. But a customer's subjective preferences or wishes are not the controlling consideration for purposes of determining whether information has been voluntarily conveyed in the first instance for purposes of the third-party doctrine. Again, as the Supreme Court noted in *Miller*, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 425 U.S. at 443.

Defendant insists that the cell-site location information acquired by the Government was too intrusive because the Government acquired records for a period of about 22 days. But this kind of durational argument furnishes little ground for a workable constitutional limitation in terms of numbers of days. Is 3 days too much? What about 15 days? Or 90 days? In *Miller*, the Government lawfully acquired all of the defendant's banking records from several accounts at two different banks for a period of *three months* without running afoul of the Fourth Amendment. *See* 425 U.S. at 437. Nor did the *Miller* court discuss the time duration, most likely because the duration of third-party disclosure is not material to whether there exists a reasonable expectation of privacy.

All that said, the critics of the third-party doctrine have strong arguments it does not adequately protect privacy—that it imposes an unacceptable and Orwellian cost of forfeiture of any claim of privacy to what we voluntarily disclose even in confidence to one another. The critics persuasively argue that the doctrine is especially problematic in our ever expanding technology-dependent and technology-intrusive society. But these are arguments for policymakers in Congress to consider, if Congress wishes to enact protections that exceed the

Fourth Amendment baseline. Or these are arguments for the Supreme Court itself to address if the high court should decide that its decisions in *Miller* and *Smith* warrant reconsideration or refinement in light of changing societal expectations of privacy.⁵

In the meantime, the obligation remains for the lower courts to follow the law and not to impose—no matter how techno-intellectually fashionable—an "everything is different because it's an iPhone" theory of the Fourth Amendment. This case is controlled by the Supreme Court's rulings in *Miller* and *Smith*.

In any event, even if I were to agree with defendant that the requirements of the Fourth Amendment applied here and "trump" the less demanding requirements of the Stored Communication Act, this would not warrant the remedy of suppression in this case, because it is apparent in light of the abundant case law in the Government's favor that the Government has relied in good faith on its authority to obtain the information in accordance with the requisites of the Stored Communications Act. *See Illinois v. Krull*, 480 U.S. 340, 348-49 (1987) (declining to apply exclusionary rule where government actors relied in good faith on authorizing statute); *United States v. Mack*, 2014 WL 6085306, at *2-*3 (D. Conn. 2014) (exclusion of cell site location information not warranted because government "was objectively reasonable in relying on the legal standard set out in Section 2703(d) when seeking [defendant's] cell site data").

Defendant further argues that suppression is warranted because the Government did not make an adequate showing of specific and articulable facts as required for a disclosure order under the Stored Communications Act. I do not agree. 6 Moreover, even if the Government's

⁵ At least one Justice appears ready to do so. *See Jones*, 132 S. Ct. at 957 (suggesting that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" and that "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks") (Sotomayor, J., concurring).

⁶ Defendant contends that the Government's application mischaracterizes a statement by a cooperating witness in this case to the effect that defendant instructed the cooperating witness to divert a narcotics shipment to

factual showing were deficient, it is well established that suppression is not a remedy that is authorized for a statutory violation of the Stored Communications Act. *See*, *e.g.*, *United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 1548 (2015).

CONCLUSION

For the foregoing reasons, the motion to suppress (Doc. #308) is DENIED.

It is so ordered.

Dated at New Haven this 24th day of February 2016.

/s/ Jeffrey Alker Meyer

Jeffrey Alker Meyer United States District Judge

Cleveland, when in fact the cooperating witness was not certain that it was defendant who instructed him to do so. Doc. #308-1 at 4. Even assuming that the application were mistaken in this respect, it is clear to me that this discrepancy was not material to a determination that there were specific and articulable facts implicating defendant in narcotics trafficking activity on the basis of extensive additional information detailed in the application.