

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

RAYMOND LAMBIS,

Defendant.

:
:
:
:
:
:
:
:
:
:

15cr734

OPINION & ORDER

WILLIAM H. PAULEY III, District Judge:

Raymond Lambis moves to suppress narcotics and drug paraphernalia recovered by law enforcement agents in connection with a search of his apartment. Lambis’s motion to suppress is granted.

BACKGROUND

In 2015, the Drug Enforcement Administration (the “DEA”) conducted an investigation into an international drug-trafficking organization. As a part of that investigation, the DEA sought a warrant for pen register information and cell site location information (“CSLI”) for a target cell phone. Pen register information is a record from the service provider of the telephone numbers dialed from a specific phone. CSLI is a record of non-content-based location information from the service provider derived from “pings” sent to cell sites by a target cell phone. CSLI allows the target phone’s location to be approximated by providing a record of where the phone has been used.

Using CSLI, DEA agents were able to determine that the target cell phone was located in the general vicinity of “the Washington Heights area by 177th and Broadway.” (April 12, 2016 Suppression Hearing Transcript (“Supp. Tr.”), at 39.) However, this CSLI was not precise enough to identify “the specific apartment building,” much less the specific unit in the

apartment complexes in the area. (Supp. Tr. at 39.)

To isolate the location more precisely, the DEA deployed a technician with a cell-site simulator to the intersection of 177th Street and Broadway. A cell-site simulator—sometimes referred to as a “StingRay,” “Hailstorm,” or “TriggerFish”—is a device that locates cell phones by mimicking the service provider’s cell tower (or “cell site”) and forcing cell phones to transmit “pings” to the simulator. The device then calculates the strength of the “pings” until the target phone is pinpointed. (See Supp. Tr. at 40.) Activating the cell-site simulator, the DEA technician first identified the apartment building with the strongest ping. Then, the technician entered that apartment building and walked the halls until he located the specific apartment where the signal was strongest. (Supp. Tr. at 41.)

The cell-site simulator identified Lambis’s apartment as the most likely location of the target cell phone. That same evening, DEA agents knocked on Lambis’s apartment door and obtained consent from Lambis’s father to enter the apartment. (Supp. Tr. at 8–9.) Once in the apartment, DEA agents obtained Lambis’s consent to search his bedroom. (Supp. Tr. at 13.) Ultimately, the agents recovered narcotics, three digital scales, empty zip lock bags, and other drug paraphernalia. (Supp. Tr. at 14.) Lambis seeks to suppress this evidence.

DISCUSSION

I. Fourth Amendment Search

The Fourth Amendment guarantees that all people shall be “secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. CONST. amend. IV. “[T]he underlying command of the Fourth Amendment is always that searches and seizures be reasonable.” New Jersey v. T.L.O., 469 U.S. 325, 337 (1985). “[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that

society recognizes as reasonable.” Kyllo v. United States, 533 U.S. 27, 33 (2001). Barring a few narrow exceptions, “warrantless searches ‘are per se unreasonable under the Fourth Amendment.’” City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)). The home has special significance under the Fourth Amendment. “‘At the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’” Kyllo, 533 U.S. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

In Kyllo, the Supreme Court held that a Fourth Amendment search occurred when Government agents used a thermal-imaging device to detect infrared radiation emanating from a home. 533 U.S. at 40. In so holding, the Court rejected the Government’s argument that because the device only detected “heat radiating from the external surface of the house,” there was no “search.” Kyllo, 533 U.S. at 35. The Court reasoned that distinguishing between “off-the-wall” observations and “through-the-wall surveillance” would “leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home.” Kyllo, 533 U.S. at 35–36. Thus, the Court held that “[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.” Kyllo, 533 U.S. at 40.

Here, as in Kyllo, the DEA’s use of the cell-site simulator to locate Lambis’s apartment was an unreasonable search because the “pings” from Lambis’s cell phone to the nearest cell site were not readily available “to anyone who wanted to look” without the use of a cell-site simulator. See United States v. Knotts, 460 U.S. 276, 281 (1983); see also State v. Andrews, 227 Md. App. 350, *23 (Md. Ct. Spec. App. 2016) (holding that the use of a cell site

simulator requires a search warrant based on probable cause, and finding that the trial court properly suppressed evidence obtained through the use of the cell-site simulator). The DEA's use of the cell-site simulator revealed "details of the home that would previously have been unknowable without physical intrusion," Kyllo, 533 U.S. at 40, namely, that the target cell phone was located within Lambis's apartment. Moreover, the cell-site simulator is not a device "in general public use." Kyllo, 533 U.S. at 40. In fact, the DEA agent who testified at the hearing had never used one.

The Government counters that Kyllo is not implicated here. In Kyllo, the Court expressed concern that the Government could employ devices, like a thermal imaging device, to learn more intimate details about the interior of the home, such as "at what hour each night the lady of the house takes her daily sauna and bath." Kyllo, 533 U.S. at 38. The Government contends that because the only information to be gleaned from a cell-site simulator is the location of the target phone (for which the Government had already obtained a warrant for CSLI), no intimate details of the apartment would be revealed and Lambis's expectation of privacy would not be implicated. But the Second Circuit has rejected a similar argument even when the search at issue could "disclose only the presence or absence of narcotics" in a person's home. United States v. Thomas, 757 F.2d 1359, 1366–67 (2d Cir. 1985) (holding that a canine sniff that "constitutes a search under the Fourth Amendment . . . when employed at a person's home").

The Government attempts to diminish the power of Second Circuit precedent by noting that Thomas represents a minority position among circuit courts. But this Court need not be mired in the Serbonian Bog of circuit splits. An electronic search for a cell phone inside an apartment is far more intrusive than a canine sniff because, unlike narcotics, cell phones are neither contraband nor illegal. In fact, they are ubiquitous. Because the vast majority of the

population uses cell phones lawfully on a daily basis, “one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful.” Kyllo, 533 U.S. at 38; see also United States v. Jacobsen, 466 U.S. 109, 124 (1984) (“[T]he reason [a canine sniff of luggage at the airport does] not intrude upon any legitimate privacy interest was that the governmental conduct could reveal nothing about noncontraband items.”).

The Supreme Court adopted a similar rationale in United States v. Karo, 468 U.S. 705, 717 (1984). There, the Court held that “[t]he monitoring of a beeper in a private residence, a location not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.” Karo, 468 U.S. at 706. The Government argued that “it should be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper wherever it goes is likely to produce evidence of criminal activity.” Karo, 468 U.S. at 717. In rejecting the Government’s argument, the Court explained that “[t]he primary reason for the warrant requirement is to interpose a neutral and detached magistrate between the citizen and the officer engaged in the often competitive enterprise of ferreting out crime,” and that “[r]equiring a warrant will have the salutary effect of ensuring that use of beepers is not abused, by imposing upon agents the requirement that they demonstrate in advance their justification for the desired search.” Karo, 468 U.S. at 717 (quotations omitted). Thus, even though the DEA believed that the use of the cell-site simulator would reveal the location of a phone associated with criminal activity, the Fourth Amendment requires the Government to obtain a warrant from a neutral magistrate to conduct that search.

The fact that the DEA had obtained a warrant for CSLI from the target cell phone does not change the equation. “If the scope of the search exceeds that permitted by the terms of

a validly issued warrant . . . , the subsequent seizure is unconstitutional without more.” Horton v. California, 496 U.S. 128, 140 (1990); see also United States v. Voustianiouk, 685 F.3d 206, 212 (2d Cir. 2012). Here, the use of the cell-site simulator to obtain more precise information about the target phone’s location was not contemplated by the original warrant application. If the Government had wished to use a cell-site simulator, it could have obtained a warrant. See Karo, 468 U.S. 705, 718 (“The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.”). And the fact that the Government previously demonstrated probable cause and obtained a warrant for CSLI from Lambis’s cell phone suggests strongly that the Government could have obtained a warrant to use a cell-site simulator, if it had wished to do so.

The use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of Kyllo. Absent a search warrant, the Government may not turn a citizen’s cell phone into a tracking device. Perhaps recognizing this, the Department of Justice changed its internal policies, and now requires government agents to obtain a warrant before utilizing a cell-site simulator. See Office of the Deputy Attorney General, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, 2015 WL 5159600 (Sept. 3, 2015); Deputy Assistant Attorney General Richard Downing Testifies Before House Oversight and Government Reform Committee at Hearing on Geolocation Technology and Privacy, 2016 WL 806338 (Mar. 2, 2016) (“The Department recognizes that the collection of precise location information in real time implicates different privacy interests than less precise information generated by a provider for its business purposes.”).

II. Fourth Amendment Considerations

The Government argues that, even if the use of the cell-site simulator constituted

a Fourth Amendment “search,” exceptions apply. The Government contends that any taint arising from the search dissipated when the agents gained consent to enter the apartment. The Government also argues that there was no reasonable expectation of privacy under the “third party doctrine.”

A. *The Attenuation Doctrine*

Under the attenuation doctrine, “[e]vidence is admissible when the connection between unconstitutional police conduct and the evidence is remote or has been interrupted by some intervening circumstance.” Utah v. Strieff, --- S. Ct. ----, 2016 WL 3369419, at *5 (June 20, 2016). In applying the doctrine, courts must determine whether the evidence at issue “was come at by exploitation of that [unconstitutional conduct] or instead by means sufficiently distinguishable to be purged of the primary taint.” Wong Sun v. United States, 371 U.S. 471, 488 (1963). The Government maintains that the seizure of evidence from Lambis’s apartment was sufficiently attenuated to dissipate the taint from any Fourth Amendment violation because the agents obtained consent from Lambis’s father to enter the apartment and obtained consent from Lambis himself to search his bedroom.

However, “the procurement of a ‘voluntary’ consent to search based upon a prior illegal search may taint the consent.” United States v. Tortorello, 533 F.2d 809, 815 (2d Cir. 1976) (citing United States v. Hearn, 496 F.2d 236 (6th Cir. 1974)). “When consent to search is preceded by an unlawful [Fourth Amendment violation], the evidence obtained from the search must ordinarily be suppressed unless the Government shows both that the consent was voluntary and that ‘the taint of the initial [seizure] has been dissipated.’” United States v. Murphy, 703 F.3d 182, 190 (2d Cir. 2012) (quoting United States v. Snype, 441 F.3d 119, 132 (2d Cir. 2006)); see also United States v. Cordero-Rosario, 786 F.3d 64, 76–77 (1st Cir. 2015) (“[C]ourts must

determine whether the causal link between a prior unlawful search and consent (voluntary though it may have been) to a subsequent search is so tight that the evidence acquired pursuant to that consent must be suppressed [T]he fact that the prior unlawful searches by the . . . police led . . . to a . . . party who then consented does not in and of itself show that the taint and exploitation concern simply disappears.”); United States v. Washington, 387 F.3d 1060, 1072 n.12 (9th Cir. 2004) (“For purposes of the Fourth Amendment, a determination that a consent was voluntarily made only satisfies a threshold requirement. The mere fact of voluntariness does not mean that a consent is not tainted by a prior Fourth Amendment violation.”) (internal quotation marks and citations omitted).

Because the Government obtained consent to enter and search the apartment, the analysis focuses on whether the Fourth Amendment violation was sufficiently attenuated such that obtaining the consent was not an exploitation of the unlawful search. To evaluate attenuation, courts consider four factors: (1) whether the defendant was given Miranda warnings, (2) the temporal proximity of the illegal action to the alleged consent, (3) the presence of intervening circumstances, and (4) the purpose and flagrancy of the official misconduct.¹ Snype, 441 F.3d at 132 (citing Kaupp v. Texas, 538 U.S. 626, 633 (2003)); see also Strieff, 2016 WL 3369419, at *5. Balancing the relevant factors, this Court determines that they weigh in favor of suppression.

The “temporal proximity” factor weighs strongly in favor of suppression. In evaluating this factor, the pertinent question is whether there was sufficient intervening time “to break the chain of illegality.” United States v. Ceballos, 812 F.2d 42, 50 (2d Cir. 1987); Murphy, 703 F.3d at 191. Courts “decline[] to find that this factor favors attenuation unless

¹ The first factor is irrelevant to this analysis as consent was not given while the party was in custody. See Snype, 441 F.3d at 134.

‘substantial time’ elapses.” Strieff, 2016 WL 3369419, at *6 (quoting Kaupp, 538 U.S. at 633); see also Brown v. Illinois, 422 U.S. 590, 604 (1975) (finding suppression appropriate where the search occurred “less than two hours” after unconstitutional arrest). Here, the DEA’s technician used the cell-site simulator on “the evening of August 27, 2015” (Supp. Tr. at 7) and the agents knocked on Lambis’s door at “[a]pproximately 8:00 p.m.” of the same evening (Supp. Tr. at 8). In the time leading up to the agents’ knock on the apartment door, the technician had to scan the streets surrounding Lambis’s apartment complex to identify the correct building and then scan each hallway of the building to identify Lambis’s apartment. (Supp. Tr. at 41.)

Based on these facts, this Court finds that the “chain of illegality” was not broken for two reasons. First, although the record is not clear as to the exact amount of time that elapsed between the violation and the consent, the two events were in close temporal proximity. And at least some portion of any time lapse could be attributable to the need for the technician to convey the cell-site simulator results to DEA agents, who then had to come up to the apartment from the street. Second, a surreptitious Fourth Amendment violation should reasonably extend the time necessary to dissipate the taint. Because neither Lambis nor his father were aware of the DEA’s use of the cell-site simulator, the DEA could have taken their time in securing consent without much risk that Lambis would dispose of the contraband.

Similarly, the “intervening circumstances” factor supports suppression: no intervening circumstances occurred between the use of the cell-site simulator and the consent to search. As Agent Glover explained, the cell-site simulator led the agents to Lambis’s apartment, where they knocked on the door and obtained consent to enter. (Supp. Tr. at 41–42.) Thus, the consent was obtained as a direct result of the illegal Fourth Amendment search and was tainted. Cf. Strieff, 2016 WL 3369419, at *8 (finding intervening circumstance in a valid arrest warrant

that “predated [the officer’s] investigation[] and . . . was entirely unconnected with the [unlawful] stop.”).

The Sixth Circuit addressed an analogous situation in Hearn. There, the police obtained a search warrant to locate a stolen bulldozer on the defendant’s farm. When they arrived at the farm, the defendant was not present. After locating the bulldozer in the first outbuilding they searched, the police then exceeded the scope of the warrant by going on to search a barn 150 yards away. There, the police located a stolen traxcavator. Hearn, 496 F.2d at 239. When the defendant appeared on the scene, police asked him to consent to a search of the barn. Unaware that the police had already entered the barn and discovered the traxcavator, defendant consented to the search. Hearn, 496 F.2d at 242.

The Sixth Circuit held that “information gained by law enforcement officers during an illegal search cannot be used in a derivative manner to obtain other evidence” and set aside the conviction of the defendant on the count relating to the stolen traxcavator. Hearn, 496 F.2d at 244; see also United States v. Hernandez, 279 F.3d 302 (5th Cir. 2002) (prior illegal “squeezing” of defendant’s luggage while in luggage compartment of bus, although unknown to defendant, taints subsequent consent because the officer “became sufficiently suspicious to engage [defendant] in conversation” in order to obtain consent to a full search of the luggage); United States v. Cordero-Rosario, 786 F.3d 64, 77 (1st Cir. 2015) (finding relevant “whether absent the illegal search, the investigators would have known the identity of all of the third parties or what to ask them.”) (citation and quotations omitted)); United States v. Politano, 491 F. Supp. 456, 463 (W.D.N.Y. 1980) (“[T]he request by Agent Peterson to see the money could only be based upon the information obtained through the prior illegal search at the airport checkpoint by the security personnel and the Cheektowaga police officer.”); LaFave, Wayne R.,

Search and Seizure: A Treatise on the Fourth Amendment, § 8.2(d) (5th ed.) (noting that exploitation of a Fourth Amendment violation “may occur by the police taking advantage of earlier illegal acts which are unknown to the consenting party and thus could not have had a coercive effect upon him.”) (emphasis in original). Accordingly, the consent obtained by the agents, however voluntary, remained tainted by the Fourth Amendment violation.

The only factor militating in favor of the Government is the “purpose and flagrancy” factor. The Second Circuit has approvingly noted that its “sister circuits have held that purposeful and flagrant police misconduct exists where ‘(1) the impropriety of the official’s misconduct was obvious or the official knew, at the time, that his conduct was likely unconstitutional but engaged in it nevertheless; and (2) the misconduct was investigatory in design and purpose and executed in the hope that something might turn up.’” United States v. Murphy, 703 F.3d 182, 192 (2d Cir. 2012) (quoting United States v. Fox, 600 F.3d 1253, 1261 (10th Cir. 2010)). The DEA agents did not intentionally commit any misconduct. However, the search, “both in design and in execution, was investigatory,” Brown, 422 U.S. at 605, and its purpose was clear: identify the apartment unit containing the target phone. As such, this factor only weighs weakly in favor of admission.

B. *The Third Party Doctrine*

Finally, the Government argues for the application of the “third party doctrine.” This Court need not address whether the third party doctrine 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,” United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayer, J., concurring), because even under the historic framework of the doctrine, it is not available to the Government here. The doctrine applies when a party “voluntarily turns over [information] to

third parties.” Smith v. Maryland, 442 U.S. 735, 744 (1979); Hoffa v. United States, 385 U.S. 293 (1966) (finding third party doctrine applicable where defendant voluntarily turned over information to Government agent). For instance, in Smith, the Supreme Court found that pen register information is subject to the third party doctrine because “[a]ll telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” Smith, 442 U.S. at 742. However, the location information detected by a cell-site simulator is different in kind from pen register information: it is neither initiated by the user nor sent to a third party.

First, “[c]ell phone users do not actively submit their location information to their service provider.” Andrews, 227 Md. App 350 at *25. “When a cell phone is powered up, it acts as a scanning radio, searching through a list of control channels for the strongest signal. The cell phone re-scans every seven seconds or when the signal strength weakens, regardless of whether a call is placed.” In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005). These “pings” are sent automatically by the phone to maintain its connection to the network. While the Second Circuit has yet to address whether these passive, CSLI “pings” fall outside the protections of the Fourth Amendment under the third party doctrine,² other Circuits have concluded that they do. See United States v. Graham, No. 12-4659, --- F.3d ----, 2016 WL 3068018 (4th Cir. May 31, 2016); United States v.

² In an unpublished opinion, the Second Circuit hinted that if presented with the question, it may find that CSLI is not protected by the Fourth Amendment. See United States v. Pascual, 502 F. App’x 75, 80 (2d Cir. 2012) (reviewing under a plain error standard because issue was not raised below and finding that “[i]t certainly was not plain error for the district court not to anticipate this innovative argument and sua sponte exclude the evidence, when no governing precedent from this Court or the Supreme Court required exclusion, and the general principles adopted by those courts pointed the other way”). Courts within the Circuit have tended to find CSLI exempt from the Fourth Amendment. See United States v. Serrano, No. 13-cr-58 (KBF), 2014 WL 2696569, at *7 (S.D.N.Y. June 10, 2014). But see In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (“[A]n exception to the third-party-disclosure doctrine applies here because cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records.”).

Carpenter, No. 14-1572, 2016 WL 1445183 (6th Cir. Apr. 13, 2016); United States v. Davis, 785 F.3d 498 (11th Cir. 2015); In re U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013). But see In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to Gov’t, 620 F.3d 304, 317 (3d Cir. 2010) (“A cell phone customer has not ‘voluntarily’ shared his location information with a cellular provider in any meaningful way.”); Tracey v. State, 152 So. 3d 504 (Fla. 2014); and State v. Earls, 214 N.J. 564, 583, 70 A.3d 630, 641 (N.J. 2013).

Nevertheless, the arguments that can be made for the application of the third party doctrine to CSLI do not extend to the distinct technology used by a cell-site simulator, which has an additional layer of involuntariness. Unlike CSLI, the “pings” picked up by the cell-site simulator are not transmitted in the normal course of the phone’s operation. Rather, “cell site simulators actively locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed.” Andrews, 227 Md. App. 350 at *3 n.4 (emphasis added); State v. Tate, 357 Wis. 2d 172, 182 n.8 (Wis. 2014); Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 2 (Sept. 3, 2015), available at <https://www.justice.gov/opa/file/767321/download>; Brian L. Owsley, Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions, 66 HASTINGS L.J. 183, 192 (2014) (“[T]here is a vulnerability in the authentication process that enables cell site simulators . . . to breach the system. . . . In other words, the cell site simulator tricks the nearby cell phone into transmitting information to it as it would the nearest cell tower.”). The involuntariness of this act is further confirmed by the fact that when the user is actively accessing the network, i.e., placing a call, “the cell site simulator will not be able to access the phone.” Andrews, 227 Md. App. 350 at *25. (See also May 23, 2016 Post-

Suppression Hearing Conference Transcript, at 12 (“[I]t is true that when a person is actually speaking into the phone, our cell site simulator cannot send or receive the ping from that phone.”).)

Second, unlike pen register information or CSLI, a cell-site simulator does not involve a third party. “Th[e] question of who is recording an individual’s information initially is key.” In re U.S. for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013) (distinguishing between “whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information”). For both pen register information and CSLI, the Government ultimately obtains the information from the service provider who is keeping a record of the information. With the cell-site simulator, the Government cuts out the middleman and obtains the information directly. Without a third party, the third party doctrine is inapplicable.

CONCLUSION

Lambis’s motion to suppress the evidence recovered by DEA agents from his apartment is granted. The Clerk of Court is directed to terminate the motion pending at ECF No. 19.

Dated: July 12, 2016
New York, New York

SO ORDERED:


WILLIAM H. PAULEY III
U.S.D.J.