IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 07-524M
	)	
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER DIRECTING A PROVIDER OF ELECTRONIC COMMUNICATIONS SERVICE TO DISCLOSE RECORDS TO THE GOVERNMENT	)	

BRIEF OF AMICUS CURIAE FEDERAL PUBLIC DEFENDER

As the Court might expect, the Federal Public Defender ("FPD") urges affirmance of Judge Lenihan's Opinion and Order denying the government's Application for a court order to seize cell site location information ("CSLI") on a showing of less than probable cause. See In Re Application of United States for an Order Directing a Provider of Electronic Communications Service to Disclose Records, 534 F.Supp.2d 585 (W.D.Pa. 2008) ("Opinion"). Judge Lenihan's conclusion that CSLI cannot be obtained absent a showing of probable cause is the only resolution of the issues at stake in these proceedings that can protect the privacy rights of all citizens, including putative defendants, here in the Western District of Pennsylvania and beyond. Because CSLI is among the most invasive of law enforcement tools – providing the government with the ability to track and with surreptitious access to constitutionally protected spaces such as one's home, one's pocket or one's person – courts must apply the most stringent standard to

ensure the reasonableness of any seizure of CSLI.

Because the FPD seeks the most protective approach (as well as a suppression remedy for illegal seizures), it concurs with the statutory and constitutional arguments presented in the Brief of Amicus Curiae The Electronic Frontier Foundation ("EFF"), The American Civil Liberties Union ("ACLU"), The ACLU-Foundation of Pennsylvania, Inc. ("ACLU of Pennsylvania"), and The Center for Democracy and Technology ("CDT") ("EFF Amici"). The FPD understands how Judge Lenihan (and other courts) reached the conclusion that the government's access to CSLI is not governed by the Stored Communications Act ("SCA") because CSLI turns a cell phone into a "tracking device," as defined by 18 U.S.C. § 3117.[1] See Opinion at 602 & n. 44. It is a plausible interpretation of the statutes involved, as CSLI obviously shares qualities with tracking devices and the government clearly intends to use the CSLI as a tracking mechanism.

However, the FPD shares the concerns of EFF Amici that such a conclusion would leave CSLI less protected. As EFF Amici point out, neither § 3117 nor Federal Rule of Criminal Procedure 41 require the government to establish probable cause or to obtain a

[1] The Electronic Communications and Privacy Act of 1984 ("ECPA") excludes "any communication from a tracking device (as defined by § 3117 of this title)" from the definition of "electronic communication." 18 U.S.C. § 2510(12)(C).

warrant before installing a tracking device.[2] EFF Brief at 10-12. So, although the FPD agrees with Judge Lenihan and other courts which have found that the government's proposed used of CSLI shares many attributes with tracking devices – and may, in fact, turn a cell phone into a tracking mechanism – it does not agree that CSLI is excluded from protection under the SCA and that the government's access thereto is governed solely by § 3117 and Rule 41.[3]

The FPD agrees with EFF Amici that this Court need not decide whether the government's proposed use of CSLI here turns a cell phone into a tracking device, as defined under § 3117. EFF Brief at 7. There are thorough and persuasive opinions on each side of the "tracking device" issue, and both Judge Lenihan and EFF Amici have thoroughly surveyed the statutory landscape for the Court in this matter. To affirm Judge Lenihan's ultimately correct

---

[2] Moreover, where the government does not comply with the requirements of § 3117, the exclusionary rule may not bar admission of any evidence acquired. See United States v. Forest, 355 F.3d 942, 950 (6th Cir. 2004), vacated on other at Garner v. United States, 543 U.S. 1100 (2004).

United States v. Gbemisola, 225 F.3d 753, 760 (D.C. Cir. 2000).

[3] It is clear that those courts which have concluded that CSLI is excluded from the SCA and is instead governed solely by § 3117 and Rule 41 did so because they understood § 3117 and Rule 41 to be more protective. See Opinion at 602-07 & ns. 41, 44. They failed to appreciate what Judge Lenihan has recognized: that the SCA, by employing the phrase "only if" in § 2703(d), provides a means to properly protect CSLI by giving courts the power to reject a request for CSLI under § 2703(d) on a showing of less than probable cause and require the government to seek a warrant. See Opinion at 608-09.

conclusion – that a warrant based on probable cause is required before CSLI can be seized – and provide the required protection, this Court need only find that CSLI remains protected under the SCA, irrespective of it tracking device qualities, as EFF Amici argue, and that Judge Lenihan correctly interpreted § 2703(d) to require the government to obtain a warrant under Rule 41 before it can seize CSLI.

The FPD need not reiterate what both Judge Lenihan and EFF Amici have so ably explained about the reasons supporting such an interpretation, but it does agree that § 2703(d)'s use of the phrase "only if" plainly authorizes a court to deny a court order for CSLI if all the government offers is "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." § 2703(d); See Opinion at 608-09; EFF Brief at 14-17.

Not only does Judge Lenihan's interpretation of § 2703(d) reflect its plain language, it is, as she found and as EFF Amici argue, compelled by the doctrine of constitutional avoidance because ascribing the meaning urged by the government would raise serious doubts about the statute's constitutionality. See Opinion at 611; EFF Brief at 17. The application of constitutional avoidance as a means of statutory interpretation does not require

a court to find that the constitution requires a certain interpretation; nor does it require a court to find that a different reading would necessarily create a constitutional violation. See United States v. Christensen, 456 F.3d 1205, 1207 (10th Cir. 2006). Constitutional avoidance is appropriately employed whenever a court concludes that a different reading of a statute might violate the constitution. Id.

Here, however, the FPD agrees with Judge Lenihan and with EFF Amici that adopting the government's reading of § 2703(d) would, in fact, create a constitutional violation because the CSLI sought here is protected under the Fourth Amendment and cannot be obtained absent a warrant based on probable cause. See Opinion at 611-16; EFF Brief at 18-31. The FPD further agrees with EFF Amici that, because there appears to be no suppression remedy available under ECPA and the SCA, See United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) (collecting cases), once a court decides the government cannot obtain a court order on a showing of less than probable cause, the correct procedure would be to deny an order under 2703(d) and require the government to seek a warrant under Rule 41. See EFF Brief at 14.

In addition to the persuasive constitutional arguments presented by EFF Amici, the FPD notes that long-standing, traditional Fourth Amendment standards applied to the facts here require a finding that a court order for the seizure of CSLI cannot

be obtained based on nothing more than "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." § 2703(d).

The "specific and articulable facts" standard contained in § 2703(d) is even less exacting than the reasonable suspicion standard, which permits law enforcement officers to briefly seize individuals without probable cause when the officer has a reasonable belief, based on specific and articulable facts and rational inferences from those facts, that criminal activity may be afoot. Illinois v. Wardlow, 528 U.S. 119, 123 (2000). An officer cannot frisk individuals they've seized unless they also can articulate specific facts that, taken together with rational inferences from those facts, point to the objective conclusion that the suspect is armed. United States v. Focareta, 2008 WL 2470912 *4 (3d Cir. 2008) (citing Terry v. Ohio, 392 U.S. 1, 21-22 (1968); Wardlow, 528 U.S. at 123-24). "Terry requires two separate sets of articulable facts-one justifying the stop and one justifying the frisk. After a valid stop, the officer may conduct a protective frisk of the suspect's outer clothing if the officer has a reasonable belief that the suspect might be armed and presently dangerous." Id. (citing Terry, 392 U.S. at 27, 30).

Under this familiar standard which, again, is more stringent

that the standard urged by the government here, an officer cannot reach into a pocket or purse and remove a cell phone even when he reasonably and objectively believes someone is engaging in criminal activity. Indeed, an officer cannot even pat down a person's outer clothing unless the officer reasonably believes the person might be armed and presently dangerous.

The government's reading of § 2703 would permit it surreptitiously to obtain access to constitutionally protected spaces on a showing of less than reasonable suspicion, when an officer armed with reasonable suspicion could not, consistent with the Fourth Amendment, access the very same spaces absent probable cause.[4] Not only does consideration of the United States Supreme Court's decisions in Kyllo v. United States, 533 U.S. 27 (2001) United States v. Karo, 468 U.S. 705 (1984), United States v. Knotts, 460 U.S. 276 (1983), Smith v. Maryland, 442 U.S. 735 (1979), United States v. Miller, 425 U.S. 435 (1976), compel the conclusion that CSLI is constitutionally protected, as EFF Amici argue, see EFF Brief at 18-31, the government's contention that a court is required to issue an order under § 2703(d) based solely on "specific and articulable facts showing that there are reasonable

[4] The government's suggestion that the seizure of CSLI does not violate the right to privacy because CSLI is so imprecise that it cannot tell if it is tracking someone in a protected space ignores the fact that the person is a protected space, as are a person's effects. U.S.CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . .").

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" is otherwise untenable when considered in light of the restrictions imposed under the well-settled Fourth Amendment standards discussed above.

* * *

Finally, the FPD notes several aspects of the government's Application it believes deserve the Court's attention. First, in its Response to Amici Motion to Unseal, the government pointed out that there is no disagreement about whether its Application seeks "historical" (stored) or "prospective" (real-time) CSLI. Government Response at 1-3. Although the FPD agrees with the government that Judge Lenihan understood its Application sought only historical CSLI, Judge Lenihan also correctly found there to be no constitutionally significant difference between historical and prospective CSLI and that delayed disclosure did not meaningfully diminish the privacy and associational interests implicated by the government's seizure of CSLI. Opinion at 612. As both Judge Lenihan's Opinion and EFF Amici's brief demonstrate, the seizure of any CSLI – historical or prospective – on a showing of less than probable cause violates the constitution. Opinion at 611-13; EFF Brief at 18-31.

The FPD notes, however, that it is impossible to glean from

the redacted Application whether the government is seeking an order that would permit seizure of CSLI for dates in the future (after it has been stored), or whether it is seeking an order to allow the seizure of already-stored CSLI for dates past.[5] If the government wants an order to seize the former, it is seeking "prospective" CSLI. That is, even if the CSLI will be momentarily stored prior to seizure, the government nevertheless is seeking prospective CSLI if it hopes to obtain CSLI "that is generated after the government has received court permission to acquire it." In re Application of United States for an Order Authorizing the Installation and use of a Pen Register and A Caller Identification System on Telephone Numbers, 402 F.Supp.2d 597, 599 (D.Md. 2005) ("Bredar Opinion").

Although the FPD, like Judge Lenihan, does not consider the historical/prospective distinction to be of constitutional significance, if this Court disagrees and is inclined to find, as some courts have suggested, that historical CSLI is entitled to lesser protection than prospective CSLI, see Opinion at 600 n. 42, it also should find that a government application seeking yet-to-be-stored CSLI is a request for prospective CSLI and is not fairly characterized as an application for historical CSLI.

Second, in its Memorandum of Law in Support of Request for Review, the government represents that it seeking "only the type of

[5] The requested time period was redacted from the Application that was unsealed. See Government's Redacted Application at ¶ a.

records shown in Exhibit C" – "that is, single-tower and sector records." Government's Memorandum at 25. It stresses that its Application "does not seek GPS or 'triangulation' information, which is in any event almost never available for past time periods." Id. (emphasis in original). It's Application, however, expressly requests not only the information in shown in Exhibit C – "call initiation and termination to include sectors available" – but "call handoffs." Government's Redacted Application at ¶ a.

Call handoffs occur when one cell tower hands off a call to another tower. There are soft handoffs and hard handoffs. A "soft handoff allows both the original cell-tower and the new cell-tower to temporarily service a call during the handoff . . . . With a soft handoff, the wireless call is actually carried by two or more cells simultaneously. CLAYTON, JADE, MCGRAW-HILL ILLUSTRATED TELECOM DICTIONARY 20.5.5 (4th ed. 2002). During a hard handoff, the call is only serviced by one cell-tower at a time during handoff. Id.

"When a phone is in touch with more than one tower, the service provider (or law enforcement, if given permission) can compare signals and locate the phone through a process of triangulation." Bredar Opinion at 599. Call handoff data, therefore, unquestionably qualifies as CSLI that "might enable law enforcement agents to engage in 'a process of triangulation from various celltowers,' and thereby 'track the movement of the target phone, and hence locate a suspect using that phone,'" In re

Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information And/or Cell Site Information, 396 F.Supp.2d 294, 300 (S.D.N.Y. 2005) ("Orenstein Opinion") (citations omitted), and therefore the government's Application does, indeed, seek triangulation information.

If this Court is inclined to find that CSLI which permits triangulation is afforded greater protection than CSLI which does not allow triangulation – a position the FPD does not endorse because all CSLI is entitled to full protection under the Fourth Amendment – the Court nevertheless should deny the government's Application because it is, in fact, seeking CSLI that would permit triangulation.[6] The FPD is not aware of any court that has allowed

[6] The government also seeks registration records. Redacted Application at ¶ a. It is the FPD's understanding that registration records are what lets the service provider know which tower you are nearest to when it needs to connect an incoming call to your phone. Registration CSLI provides the location of the cellphone when it is not being used, so any claim that the government will only be able to track the subject when his phone is in use is specious. Moreover, even courts which have granted government applications for CSLI have found the government cannot obtain "any cell site information that might be available when the user's cell phone was turned 'on' but a call was not in progress." Hornsby Opinion at 682-83.

From the FPD's perspective, the government's Application fails to convey critical details about the nature of CSLI sought. It should not affect the Court's resolution of the statutory and constitutional issues involved, but the FPD hopes that, irrespective of the standard to be applied, the Court will require a more precise description of the information sought before evaluating an application for CSLI.

the government to seize CSLI that permits triangulation without obtaining a warrant based on probable cause. See, e.g., In re Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information, 2007 WL 3036849 at * 3 (S.D.Tex., Oct. 17, 2007) (noting that in cases in which courts granted the applications for CSLI, the Government was not seeking . . . "to obtain information from multiple cellular antenna towers simultaneously to 'triangulate' the precise location of a cell phone"); In re Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F.Supp.2d at 448, 461 (S.D.N.Y, Oct. 23, 2006) ("permitted disclosure of prospective cell-site information, emphasizing that the Government did not seek triangulation information"); In re Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F.Supp.2d 678, 682-83 (W.D.La., Jan. 26, 2006) ("Hornsby Opinion") (holding Government could not get "information that would allow the Government to triangulate multiple tower locations and thereby pinpoint the location of the user").

The final point worth noting is that if the government's representations are correct, and the CSLI it is seeking here is so

imprecise that "only suggests an area of tens of thousands (or more) square yards large in which the target phone was used," Government Memorandum at 26, one has to question whether the government can meet § 2703(d)'s materiality requirement.

As stated above, the FPD agrees EFF Amici that the level of precision does not impact the statutory or constitutional analysis here; however, if the Court were to agree with the government that it need only establish "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" to obtain a court order under § 2703(d), it is important that the Court strictly hold the government to its burden.

In other contexts, information is material if there is a reasonable probability of a different result. See, e.g., Kyles v. Whitley, 514 U.S. 419, 434 (1995); Strickland v. Washington, 466 U.S. 668, 693 (1984). If the same definition of materiality were applied here, § 2703(d) would require the government to establish a reasonable probability that if the information sought were provided, it would then be able to locate the subject and his supplier. If the CSLI at issue here is "much too imprecise" and general that the government cannot even tell "whether calls have been made from a constitutionally protected space," Government

Memorandum at 26, it follows that such information is much too imprecise to be material to the government's efforts to locate the individuals it seeks to find.[7]

* * *

"You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinized." George Orwell, 1984 (Harcourt Brace Jovanovich 1949).

The FPD does not mean to be hyperbolic, nor signal any lack of respect for the Court or these proceedings, with its reference to Orwell's prescience. Rather, it merely seeks to underscore what is seems painfully obvious: that an open society cannot exist if the mere use of a cell phone constitutes a full relinquishment of the expectation of privacy in your person, places and effects. The logical extension of the government's argument would leave people unable to even meagerly participate in society without forfeiting their rights under the Fourth Amendment.

The government's position here is reminiscent of its position in a case out of this district about a decade ago: United States v.

---

[7] In its Supplemental Memorandum of Law in Support of Request and Review, the government advises that "at least one wireless telephone company" "generates periodic location information using so called 'pilot signals' . . . [which] may indicate the location of the mobile handset to a precision of approximately 200 meters." Government's Supplemental Memorandum at 1-2. Interestingly, the government has chosen not to seek these more precise records.

Given the government's stated desire to find the subject and his supplier, its decision to forgo the more precise CSLI is fairly interpreted as an implicit recognition that such information is not available absent a warrant based on probable cause.

McGuire, 178 F.3d 203 (3d Cir. 1999). McGuire involved the arson of catering truck and the federal arson statute's jurisdictional element requires proof beyond a reasonable doubt that "the property [truck] was used in any activity affecting interstate or foreign commerce." 18 U.S.C. § 844(i). The government secured a conviction and on appeal the defendant argued, inter alia, that the government failed to present sufficient evidence to support the interstate commerce element of the arson statute. McGuire, 178 F.3d at 206.

The government argued that a single carton of orange juice that was manufactured in Florida was sufficient to establish that the truck was "used" in interstate commerce. Id. at 208. The Court rejected the government's argument and noted that, "'in view of our complex society,' there is virtually nothing that does not affect interstate commerce in some manner." Id. at 210 (quoting United States v. Lopez, 514 U.S. 549, 567 (1995)). It ultimately found that a federal arson conviction "must rest upon more than the dubious interstate commerce nexus of our hypothetical cup of sugar, or the ephemeral nexus of the government's carton of orange juice. '[I]n view of our complex society,' supporting this conviction by so slender a thread as the government presented here would be tantamount to removing the jurisdictional requirement from § 844(I)." Id. at 211-12.

Just as the McGuire Court recognized that, "'in view of our

complex society,' there is virtually nothing that does not affect interstate commerce in some manner," id. at 210, this Court should recognize that, in our complex and technologically advancing society, there is virtually nothing a person can do that does not necessarily reveal some otherwise secreted information about herself. If the government is correct, then anyone seeking to preserve the right to privacy will simply be unable to meaningfully participate in society. That is a trade-off (and a society) this Court should refuse to endorse.

Respectfully submitted,

/s/ Lisa B. Freeland
Federal Public Defender
Amicus Curiae