UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING PROSPECTIVE AND CONTINUOUS RELEASE OF CELL SITE LOCATION RECORDS	§ § § § § § §	CRIMINAL ACTION NO. H:13-CV-1198M

OPINION

Recent case law prompts this court to confront yet again an important question of electronic surveillance law: Under what statutory authority is law enforcement permitted to continuously monitor a cell phone's location in (or near) real time?

Background

As part of a drug trafficking investigation, the government has applied for an order under § 2703(d) of the Stored Communications Act (SCA) compelling a phone company to disclose, among other information, cell site data for a target phone "on a continuous basis contemporaneous with" the beginning and end of a call, and if reasonably available, during the call as well.[1] In other words, the government seeks to compel continuous and contemporaneous access to cell phone location records not yet created for phone calls not yet made. To be clear, the government does not seek to compel the provider to

1Sealed Application ¶ 20. The full text of this request reads: "For the Target Device, after receipt and storage, records or other information pertaining to subscriber(s) or customer(s), including the means and source of payment for the service and cell site information, provided to the United States on a continuous basis contemporaneous with (a) the origination of a call from the Target Device or the answer of a call to the Target Device, (b) the termination of the call and (c) if reasonably available, during the progress of the call, but not including the contents of the communications."

generate records not ordinarily kept;[2] the requested call location data are said to be ordinary business records. No end-date for the monitoring period is stated.[3]

In the past the DOJ has invoked a "hybrid"of several statutes to support its request, but the government's application here relies solely upon the SCA. This court initially denied this part of the government request, but indicated it would consider further briefing on the issue if the government chose to submit it. No such brief was filed.

Analysis

Writing on a mostly clean slate nine years ago,[4] this court concluded that prospective monitoring of cell site data converts a cell phone into a "tracking device" under the federal Tracking Device Statute,[5] which is subject to the warrant requirements of Rule 41 of the Federal Rules of Criminal Procedure.

Since 2005, other magistrate and district judges have weighed in.[6] Some disagreed that a warrant was necessary, holding that such prospective location data is available under the lower, "specific and articulable facts" threshold of the SCA.[7] But most

2The SCA does not generally empower the government to require providers to create documents. *See In re Application*, 2007 WL 2086663, *1 (S.D. Tex. July 6, 2007).

3Presumably the monitoring would be co-extensive with the 60-day pen register accompanying this request. *See In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F.Supp.2d 876, 880 n. 7 (S.D.Tex. 2008) (explaining the government's practice in this district of seeking a combined pen/trap and 2703(d) order).

4*In re Application*, 396 F.Supp.2d 747 (S.D.Tex. 2005). The only other opinion on the topic had been issued a few months earlier by my fellow magistrate judge James Orenstein. *In re Application*, 396 F.Supp.2d 294 (E.D.N.Y. 2005).

518 U.S.C. § 3117.

6For a summary of reported cell site decisions as of June 2010, see *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 93 (2010), *available at* ssrn.com/abstract=2173529.

7*See e.g., In re Application*, 632 F.Supp.2d 202 (E.D.N.Y. 2008) (Garaufis); *In re Application*, 405 F.Supp.2d 435 (S.D.N.Y 2005) (Gorenstein).

published opinions have gone in the other direction, agreeing with this court that the SCA did not apply to real-time monitoring of cell site data.[8] The government has yet to appeal these adverse rulings beyond the district level; nevertheless, in this district it routinely requests such authority in its form applications for pen/trap/2703(d) orders. To date no federal appellate court has addressed this particular issue of ongoing surveillance under the SCA.

Last year a divided Fifth Circuit panel held that orders for historical cell site records under the SCA do not categorically violate the Fourth Amendment. *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013).[9] The court described its decision as "narrow" and expressly limited to "*historical* cell cite information for specified cell phones at the points at which the user places and terminates a call."[10] While the court did assume that historical cell site records were "covered under the plain text of [SCA] § 2703 (c),"[11] the opinion was silent about

---

8*See e.g.*, *United States v. Espudo*, 954 F.Supp.2d 1029, 1036-37 (S.D. Cal. 2013); *In re Application*, 396 F.Supp.2d at 308-09 (E.D.N.Y. 2005) (Orenstein).

9Since that time, two significant cell phone-related decisions have been handed down: *Riley v. California*, 134 S.Ct. 2473 (2014) (warrantless search of digital data on a cell phone seized incident to arrest violates Fourth Amendment), and *United States v. Davis*, 2014 WL 2599917 (11th Cir. June 11, 2014) (obtaining cell site location data without a warrant violates the Fourth Amendment).

10724 F.3d at 615 (emphasis in original).

11*Id.* at 604. None of the parties before the Fifth Circuit contested the categorization of cell site data as "a record or other information pertaining to a customer or subscriber" within the meaning of the SCA. Nor was the issue raised or decided by the lower court, which confined itself to the constitutional question. 747 F. Supp.2d 827 (S.D. Tex. 2010). However, other courts have held that the tracking device exclusion in the ECPA's definition of "electronic communication" removes cell site data from the ambit of the SCA. *See e.g.*, *In re Application*, 2009 WL 159187 (S.D.N.Y., Jan. 13, 2009) (McMahon) (citing cases). Another potentially vexing question is whether the SCA covers cell site information of a phone *user* who is neither "a customer or subscriber." *Cf. In re Application*, 415 F.Supp.2d 663, 666 (S.D.W.Va. 2006) (Stanley) (distinguishing between "user" and "subscriber" in the context of a pen register

prospective cell site data or continuous monitoring.

Even so, given law enforcement persistence in pursuing this authority, it seems appropriate to revisit our 2005 statutory holding in light of the Fifth Circuit's recent constitutional ruling. The main questions are (1) whether the SCA authorizes ongoing surveillance of cell phone use; (2) whether cell phone tracking is distinguishable from other forms of tracking covered by the Tracking Device Statute and Rule 41; and (3) whether the hybrid theory – a combination of the SCA with other statutes – offers a plausible alternative legal regime for cell phone tracking. The answer to each question is no, for reasons explained below.

1. Distinguishing Historical and Prospective Cell Site Records

The Fifth Circuit's emphasis that its holding was limited to historical cell site information begs the obvious question: what exactly *is* historical cell site information? The SCA does not define the term; in fact, the words "historical" and "cell site" are never used in the SCA. The closest the Fifth Circuit comes to a definition is the following passage: "In the case of such historical cell site information, the Government merely *comes in after the fact* and asks a provider to turn over records the provider has *already created*."[12] In other words, the records sought were historical in the sense that they were created *before* the government's request to the provider.

---

application seeking cell site location data); *see generally* Nathaniel Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1947 (2009) (The SCA "only regulates information pertaining to customers or subscribers of covered information services."). To the extent these questions remain open after the Fifth Circuit's ruling, I leave them for another day.

12724 F.3d at 612 (emphasis added).

The government's application here exceeds the scope of the one blessed by *Historical Cell Site* in two significant respects. First, the information sought here is "prospective,"[13] in the sense that law enforcement seeks disclosure of records created in the future, *after* the government's request. Second, and more importantly, the government seeks to impose a *continuing* obligation of disclosure on the provider, thereby enabling law enforcement to monitor the cell phone's call location contemporaneously in (or near) real time. Such monitoring authority is beyond the one-time access apparently contemplated in the Fifth Circuit's decision. Is it also beyond the authority conferred by the SCA?

Instantaneous storage theory. The government does not think so. In other cases, the government has vigorously challenged the viability of any distinction between "historical" and "prospective" cell site data, arguing that cell phone signaling data becomes a "record" as soon as it is captured and digitally "stored" on the provider's system. This data is historical in one sense and prospective in another: "[T]he same datum that is prospectively created by a disclosure order is a 'record' by the time that it must be turned over to law enforcement."[14] Either way, according to the government, cell site data – whenever it is created – is a transaction record subject to production under the SCA.

This argument, dubbed the "instantaneous storage" theory by Judge Orenstein in

13Strictly speaking, the term "prospective record" is an oxymoron, because there is no such thing as a record of a future event, at least in ordinary experience. *Cf.* BACK TO THE FUTURE (Universal Pictures 1985). Nevertheless, it will be used here as a convenient shorthand to distinguish those records from the historical records covered by the Fifth Circuit's decision.

14Orenstein, 396 F.Supp.2d at 312 (E.D.N.Y. 2005) (quoting government's reply brief).

the first reported cell site opinion,[15] has found a mixed reception. Some, like Judge Orenstein, have rejected it, citing the SCA's use of the present tense to describe the government's burden of showing that the requested items "*are* relevant and material to an ongoing investigation."[16] Other courts have accepted the theory, finding prospective cell site data no different in substance from historical data at the time of its transmission to the government.[17]

The instantaneous storage argument is not unreasonable, so far as it goes. The SCA does not specify a particular cut-off date for determining which records are to be produced. There are many possibilities: the date of the government's application; the date the order is signed by the judge; the date the order is served on the provider; the date the provider actually produces the records; or a different date specified by the court's order. Absent a clear dividing line to separate present from future data,[18] the distinction

---

15*Id*.

16*United States v. Espudo*, 954 F.Supp.2d 1029, 1037 (S.D.Cal. 2013); *but see* Dictionary Act, 1 U.S.C. § 1 ("[U]nless the context indicates otherwise, . . . words used in the present tense indicate the future as well as the present.").

17*See United States v. Booker*, 2013 WL 2903562, *7 (N.D. Ga. 2013) ("While this information is 'prospective' in the sense that the records had not yet been created at the time the Order was authorized, it is no different in substance from the historical cell site information . . . at the time it is transmitted to the government."); *In re Application* , 632 F.Supp.2d 202, 207 n. 8 (E.D.N.Y. 2008) (Garaufis) ("The prospective cell-site information sought by the Government . . . becomes a 'historical record' as soon as it is recorded by the provider."); *In re Application*, 460 F.Supp.2d 448, 459 (S.D.N.Y. 2006) (Kaplan) ("[T]he information the government requests is, in fact, a stored, historical record because it will be received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials."); *In re Application*, 405 F. Supp.2d 435, 444 (S.D.N.Y. 2005) (Gorenstein) (nothing in the SCA limits when "information may come into being").

18As the poet says, the present is a moving finger that "writes, and having writ, moves on." EDWARD FITZGERALD, THE RUBAIYAT OF OMAR KHAYYAM 71 (William Henry Martin & Sandra Mason, 4th ed. 1879). *See also* TENNESSEE WILLIAMS, THE GLASS MENAGERIE 96 (New Directions 2011) ("The future becomes the present, the present the past."); *cf*. WILLIAM FAULKNER, REQUIEM FOR A NUN 73 (Vintage Books 1950) ("The past is never dead. It's not

between historical and prospective cell site data becomes blurred, because digital data can morph into a record within nanoseconds after creation.

One-time access vs. continuous monitoring. Even if the government were correct that a 2703(d) order may require the provider to disclose, at some future time, documents not yet in existence when the order is issued, a much larger hurdle remains: Does the SCA impose a *continuing* obligation to disclose customer records, thereby enabling ongoing surveillance, as the government contends? Or is the provider's statutory disclosure obligation satisfied by one-time production of existing records?

The Supreme Court in *Berger v. New York* recognized a fundamental distinction between ongoing electronic surveillance and a one-time search, leading the Court to impose more stringent procedural requirements than those applicable to an ordinary search warrant.[19] The focus of the *Berger* opinion was the deficiencies of a state eavesdropping law, but appellate courts have identified similar infirmities with other forms of electronic surveillance: it is intrusive, continuous, indiscriminate, and secret. [20] As one respected commentator has elaborated:

> The hidden nature of electronic surveillance makes it more likely that an investigation will reveal private information. . . . Electronic surveillance monitors continuously, increasing the likelihood that people other than the target of the surveillance will have their private information disclosed. Even hardened criminals talk to their mothers and lovers. . . . Electronic surveillance is "indiscriminate" in the sense that it may obtain information

even past.").

19*Berger v. New York*, 388 U.S. 41, 57 (1967) ("[A]uthorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause.").

20*See e.g.*, *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987) (video surveillance); *United States v. Torres*, 751 F.2d 875, 884-85 (7th Cir. 1984) (same).

> that has no link to criminal activity. Any number of entirely innocent people may either call or be called from a wiretapped phone. Electronic surveillance casts a far wider net than a traditional search for evidence of a crime at a target's home or business. . . . Finally, electronic surveillance cannot be effective unless it is secret. . . Compared to traditional searches, . . . law enforcement agents can use electronic surveillance investigations to flout the law without notifying anyone.[21]

Mindful of these dangers, Congress has been attentive to the distinction between ongoing surveillance and one-time access when regulating law enforcement investigative techniques. Continuous search mechanisms like wiretaps, pen registers, and tracking devices are typically hemmed in by duration periods and other prospective features.[22] On the other hand, record production regimes have no need for such features because they do not involve ongoing surveillance. An administrative subpoena or a civil discovery request is typically satisfied by a one time production of documents;[23] a search warrant for records authorizes one-time access, not repeated searches of the same premises, day after day, week after week, month after month. Real time monitoring of cell site data would mark a radical departure from existing legal regimes for record production. Is there anything in the SCA to support it? The answer is plainly no.[24]

21Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 18-19 (2004).

22*See In re Application*, 396 F.Supp.2d 747, 760 (S. D. Tex. 2005)

23FED. R. CIV. P. 26(e)(1)(A) imposes a limited duty to supplement discovery responses only "if the party learns that in some material respect the disclosure or response is incomplete or incorrect." *See Reed v. Iowa Marine and Repair Corp.*, 16 F.3d 82 (5th Cir. 1994). Even then, the supplementation need not be continuous, but only "at appropriate intervals during the discovery period." Advisory Committee Note, 146 F.R.D. at 641; 8AWRIGHT, MILLER & MARCUS, FEDERAL PRACTICE & PROCEDURE § 2049.1, at 317 (4th ed. 2010).

24Some cases freely concede that the SCA by itself imposes no such obligation, but attempt to derive such an obligation by reading the SCA in combination with the Pen Register Statute, which does authorize prospective surveillance. *See e.g. In re Application*, 460 F.Supp.2d 448, 460 (S.D.N.Y. 2006) (Kaplan). This "hybrid" theory is discussed below.

The SCA is part of a comprehensive statute passed in 1986, the Electronic Communications Privacy Act. In separate titles, that law recognizes three different types of ongoing surveillance. Title I amended the Wiretap Act to include interception of electronic communications content. The same title also authorized use of tracking devices outside the district of installation, providing a broad definition of "tracking device" subsequently incorporated into Rule 41.[25] Title III authorized pen registers and trap and trace devices. What these schemes have in common are forward-looking mechanisms (e.g. duration period, renewal, reporting, minimization, and sealing) aimed at ongoing activity, not a one-time event.

Title II, referred to as the Stored Communications Act, is different. Modeled after the Right to Financial Privacy Act (RFPA) governing law enforcement access to bank records,[26] the SCA is designed to regulate government access to stored electronic communications and transaction records. Just as the RFPA does not authorize law enforcement to monitor bank account transactions as they occur in real time,[27] nothing in the SCA imposes a continuing obligation on the provider to disclose account records over time. The SCA has no monitoring periods, no extensions, no minimization requirements, no periodic reporting, no automatic sealing. In short, none of the signature elements of an ongoing surveillance scheme are present.

25See FED. R. CRIM. P 41(a)(2)(E) ("'Tracking device' has the same meaning set out in 18 U.S.C. 3117."). This definition was part of a 2006 amendment to specify procedures for issuing tracking device warrants.

26S. Rep. No. 99-541, at 3 (1986).

27*See* Susan Freiwald & Sylvain Metille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261, 1322-24 (2013) (contrasting the RFPA with Swiss law, which does permit real-time surveillance of bank transactions).

The SCA's only nod to prospective data gathering is section 2703(f), which authorizes the government to require a provider "to preserve records and other evidence in its possession pending the issuance of a court order."[28] As Judge Orenstein has rightly pointed out,[29] this mechanism allows the government to obtain future location records, albeit not contemporaneously, pursuant to a *retrospective* 2703(d) order. By using 2703(f), the government may direct the preservation of records to be disclosed later, in response to a 2703(d) order issued *after* those records are created. This mechanism for one-time access to prospective data is compelling evidence that Congress did not contemplate real-time monitoring of customer data.

In sum, as two noted scholars on the ECPA have written, "Congress never intended the Stored Communications Act to govern ongoing surveillance."[30]

2. Tracking Surveillance Under the ECPA

Separate and apart from the SCA's text, a familiar principle of statutory construction compels rejection of the government's surveillance request. As explained above, the SCA is part of a larger statute, the ECPA, and its provisions must be construed in harmony with the rest of that law. *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994) ("[W]hen construing a statute, we do not

---

2818 U.S.C. 2703(f).

29*In re Application*, 396 F.Supp.2d 294, 313 (E.D.N.Y 2005).

30Supplemental Brief for Center for Democracy and Technology, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the American Library Ass'n, Amicus Curiae Supporting Appellants, *United States v. Councilman*, 418 F.3d 67 (No. 03-1383), 2004 WL 2058257. The case involved an appeal challenging a district court order that emails in momentary electronic storage could be continuously accessed under the SCA as opposed to the Wiretap Act.

confine our interpretation to the one portion at issue, but, instead, consider the statute as a whole."). Applying that precept in its first encounter with ECPA, the *Steve Jackson* court found that Congress did not intend substantive overlap between ECPA's various titles, and held that conduct covered by the SCA (Title II) was not simultaneously covered by the wiretap provisions of Title I.[31]

Tracking Device Statute. Similarly here, continuous and contemporaneous monitoring of cell site location data is tantamount to tracking, a form of surveillance Congress separately treated in ECPA.[32] As originally drafted, the law expressly paired tracking devices and pen registers in the same title, setting forth procedures for the issuance of court orders allowing their installation and use.[33] In its final form, only two provisions dealing with tracking devices were retained: Section 3117(a), which permitted the installation of tracking devices which may move from district to district; and Section 3117(b), which broadly defined tracking device to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object."[34]

3136 F.3d at 464.

3218 U.S.C. § 3117.

33*See* H.R. 3378, 99th Cong., 1st Sess., Title II, 201. The proposed bill would have required probable cause for a tracking device order, and reasonable cause for a pen register. Legislative history suggests that these tracking devices provisions were later removed due to uncertainty over the proper constitutional standard for tracking device warrants after *U.S. v. Karo*, 468 U.S. 705 (1984). *See Electronic Communications Privacy Act: Hearing on H.R. 3378 Before Subcomm. on Courts, Civil Liberties, and Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong., 254-274 (1986) (statement of Clifford F. Fishman, Professor of Law, The Catholic University of America School of Law).

34This definition was a shorter version of that originally proposed in H.R. 3378, which read: "an electronic or mechanical device which permits the tracking of the movement of a person or object *in circumstances in which there exists a reasonable expectation of privacy with respect to such tracking.*" H.R. 3378, 99th Cong. 205 (1985) (emphasis added).

Subsequently, Congress approved amendments to Rule 41 specifying the procedural requirements for a tracking device warrant. Among those requirements are probable cause, a 45-day duration period, return to the designated magistrate judge, and notice to the targeted person.[35] Rule 41(a)(2)(E) expressly incorporates the definition of tracking device from the Tracking Device Statute. Given this detailed regime for location tracking, there is no reason to suspect that Congress ever intended the SCA to open a back door for law enforcement to employ the same surveillance technique under different (and less rigorous) standards.

It might be argued that, in theory, nothing in the SCA prevents an agent from preparing a stack of 2703(d) orders to be served one per hour, day after day, thereby accomplishing the continuous monitoring sought here. Likewise, nothing in the SCA explicitly prohibits an agent from making a similar end run around the Wiretap Act, by lining up a string of §2703(a) orders for stored emails and serving them seriatim. But, as Professor Kerr has observed, obtaining email content in this way "makes the access the functional equivalent of a wiretap, [and so] should be regulated by the Wiretap Act, not the SCA."[36] The same would hold true for serial §2703(d) orders seeking location data—as the functional equivalent of a tracking warrant, they should be regulated by Rule 41,

35FED. R. CRIM. P. 41(d)(1), (e)(2) (C), (f)(2). The Advisory Committee Notes observed that the 2006 amendments did not resolve the constitutional issue of the showing required for a tracking warrant, which was left open in *Karo*. The rule simply provides that the magistrate judge must issue the warrant if probable cause is shown, and takes no position whether something less than probable cause would suffice. This court has found no case granting a tracking warrant on less than probable cause, nor has the government ever submitted to this court a Rule 41 tracking warrant application asserting a lesser standard than probable cause.

36Orin Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L.REV. 1208, 1232-33 (2004).

not the SCA. Careful adherence to the distinction between one-time access and ongoing surveillance will, in the words of Professor Kerr, "ensure that the line between the SCA and the Wiretap Act and Pen Register statute is functional and sensible rather than incoherent and arbitrary."[37]

***Smartphone* decision.** Some courts have resisted the conclusion that the Tracking Device Statute covers prospective tracking by cell site data. While not disputing that a cell phone is a tracking device in *fact*,[38] these courts contend that a cell phone is not a "tracking device" in *law*, i.e. the Tracking Device Statute and Rule 41. This conclusion is not derived from the statutory definition of a tracking device, which neatly fits the modern cell phone: "an electronic or mechanical device which permits the tracking of the movement of a person or object."[39] Instead, several other justifications are offered, as illustrated by a recent decision, *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129 (E.D.N.Y. 2013) (Brown).

First, *Smartphone* argues that the phrase "tracking device" had a plain meaning both prior and extrinsic to the enactment of the ECPA in 1986,[40] and points to a Senate Report describing a simple transponder — state of the art tracking technology in 1986, but now obsolete.[41] The legislative history has legitimate uses in statutory construction,

37*Id.* at 1233.

38One prominent investigative journalist on the technology/privacy beat has described cell phones as "the world's most effective tracking devices, even when they are turned off." JULIA ANGWIN, DRAGNET NATION 141 (2014).

3918 U.S.C. § 3117(b); FED. R. CRIM. P. 41(a)(2)(E).

40977 F.Supp.2d at 149.

41S. Rep. 99-541, at 10 (1986). For a discussion of the evolution in tracking technology, see *United States v. Katzin*, 732 F.3d 187, 191-92 (3d Cir.), *reh'g granted*, 2013 WL 7033666 (3d Cir. Dec. 12, 2013).

but this is not one of them. When Congress unambiguously defines a term in the United States Code, a reviewing court has no power to *re*define that term based on extraneous sources of "plain meaning."[42] The descriptive passage in the Senate Report could not, and did not purport to, displace the statutory definition of "tracking device" enacted by Congress. As Judge Posner observed in a related context concerning the same report, its description of technology was merely "illustrative, not definitional."[43] Nor was Congress unaware that the definition's breadth might encompass cell phones; a prominent telecommunications executive had raised this very possibility in testimony at a committee hearing.[44] The ECPA Congress plainly understood the state of tracking technology as it then existed, and, just as plainly, drafted a technology-neutral definition to cover future advances.

Next, the *Smartphone* court points to subsection (a) of section 3117 discussing the "installation" of a mobile tracking device, and from this lone word infers that "the statute is aimed at devices installed specifically to track someone or something, as opposed to cell phones which, incidental to their intended purpose, can be tracked or traced."[45] But an "installation" in our digital age need not entail a physical process, like placing a

---

42*See* 2A N. SINGER & S. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 45.8 at 53 (7th ed. 2014) (noting that popular or received meaning of words in statute may be consulted only "in the absence of a statutory definition").

43*United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir. 1997).

44*Electronic Communications Privacy Act: Hearing on H.R. 3378 Before Subcomm. on Courts, Civil Liberties, and Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. *Hearing on HR 3378*, 99th Cong. 99 (1985). (statement of John W. Stanton, Chairman, Telelocator Network of America, and Executive Vice President, McCaw Communications Co., Inc.).

45977 F.Supp.2d at 150.

beeper under a truck bumper; as often as not the term refers to a screen tap or keystroke by which new software is electronically "installed" on digital devices.[46] Nor is it correct to assume that cell phones have a single intended purpose. As the Supreme Court recently observed in its landmark cell phone search case:

> The term "cell phone" is itself misleading shorthand: many of these devices are in fact minicomputers that also have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[47]

Or, just as easily, "the world's most effective tracking devices."[48]

Finally, the *Smartphone* opinion worries that taking the "tracking device" definition literally would lead to warrants in "illogical and unworkable" circumstances, such as bicycle tire tracks in a muddy field, or an automobile taillight, or the transmitter of a pirate radio station. But these examples are not particularly troublesome,[49] and far less so than the consequences of the opinion's own crabbed reading. Accepting *Smartphone's* premise that Congress intended § 3117(b) to refer only to 1986-vintage

---

46The Pen/Trap Statute repeatedly uses the same word, even though the modern pen register is installed electronically rather than physically. 18 U.S.C. §§3121-3125; *see also* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 S. CAL. L. REV. 949, 982-89 (1996) (describing the evolution of the pen register from mechanical device to computer system).

47*Riley v. California*, 134 S.Ct. 2473, 2489 (2014).

48*See supra* note 38.

49A bicycle wheel rut may provide evidence that something has passed, but it is no more a "mechanical or electronic device" than a footprint or the wake of a ship. A bicycle and a taillight may be devices, but neither intrinsically reveals "movement" except through direct observation, unlike a beeper or a cell phone. As for the pirate radio, the transmitter revealing its location is functionally indistinguishable from the beeper planted in the container of contraband in *Karo*, and could just as easily qualify as a tracking device.

beepers, not only would cell phones be excluded, but also current tracking technology like GPS devices. And Rule 41's tracking warrant provisions would be similarly obsolete, because they adopt the same definition of "tracking device" that Congress enacted in 1986.[50]

Smartphone does not address these anomalies, nor the larger question they pose: why, instead of a uniform and coherent legal regime for tracking devices, would Congress prefer a fragmented scheme with varying standards dependent upon the type of technology used? Multiple standards for tracking technologies (most of which rely on radio waves in some form anyway) would seem to accomplish very little for law enforcement,[51] other than to generate confusion and opportunity for manipulation, goals unworthy of Congress.

These considerations compel me to respectfully disagree with my colleague from New York, and to reject the SCA as stand-alone authority for prospective, continuous, and contemporaneous cell site monitoring. Both in fact and in law, this type of surveillance converts a smartphone into a tracking device, and it is governed by the standards of Rule 41, not the SCA.

3. Hybrid Theory

50See FED. R. CRIM. P. 41(a)(2)(E) ("'Tracking device' has the meaning set out in 18 U.S.C. § 3117(b).").

51In this district the government's practice is to invoke at least three different legal mechanisms to track a target: a SCA 2703(d) order for tracking a cell phone by single tower cell data; a "precise location" warrant based on probable cause for tracking a cell phone's precise location by GPS or triangulation and a Rule 41 tracking warrant for GPS tracking by device other than a cell phone.

If the prior analysis is correct, then the SCA is not a proper vehicle to compel continuous disclosure of *any* type of records, including cell site data. In other cases, the government has argued, with limited success, that cell site data is a special category of business records, accessible by a unique combination of statutory authorities. This "hybrid theory" posits that a 1994 law (CALEA)[52] implicitly authorized the acquisition of prospective cell site data under the combined authority of the SCA and the Pen/ Trap Statute. The most thorough elaboration of this theory to date is the 2005 opinion by Judge Gorenstein.[53] A minority of published decisions have accepted the hybrid theory,[54] relying almost entirely upon the arguments initially laid out by Judge Gorenstein. Those decisions largely ignore subsequent criticisms of his opinion,[55] so the debate has advanced very little in recent years. Unlike the Western Front commanders of a century ago, I will resist the temptation to launch yet another sortie over the same ground covered by these competing opinions. Instead, a short summary of the main unanswered questions for the hybrid theory will suffice:

• *Missing exception.* How does the hybrid theory escape the SCA's general prohibition against divulging customer records "to any governmental entity"?[56] None of the listed exceptions to that prohibition cite the Pen/Trap Statute, an omission that

---

52Communications Assistance to Law Enforcement Act, 47 U.S.C. § 1002(a)(2).

53405 F.Supp.2d 435 (S.D.N.Y. 2005).

54*See supra* note 6.

55*See e.g.*, *In re Application*, 441 F.Supp.2d 816 (S.D.Tex. 2006).

5618 U.S. C. § 2702(a)(3) ("Except as provided in subsection (b) or (c), . . . a provider of remote computing service or electronic communications service to the public shall not knowingly divulge a record or other information pertaining to a subscriber or customer of such service . . . to any governmental entity.").

effectively sinks the hybrid theory.[57]

• *Paternity.* If the SCA and the Pen/Trap Statute were indeed the parents of a new form of surveillance, why don't they seem to know each other? Neither statute mentions such a symbiotic relationship with the other, nor do their respective legislative histories hint at such a pairing.[58]

• *Birthday.* Even if these statutes had a covert one-night stand, when did the rendezvous occur? The relevant statutory provisions were passed at various times over 15 years. On none of those occasions did anyone in Congress, DOJ, industry, or academia announce (or even notice) that a new breed of electronic surveillance had been spawned.[59]

• *Congressional clairvoyance.* How did Congress know in 1994, when CALEA was passed, that seven years later the Patriot Act would amend the pen/trap definitions to include signaling information such as cell site data? Until 2001, the Pen/Trap Statute had covered only phone numbers dialed, not call location information.[60]

• *Hidden elephant.* Why would Congress by a wink and a nod create an alternative legal regime for an investigative technique — mobile tracking devices — already the subject of a specific statute and established procedures? Justice Scalia's memorable phrase is apt: "Congress, we have held, does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions — it does not, one might say,

5718 U.S.C. § 2702(c) (1)-(6). Significantly, the prohibition on divulging customer records was first added to the SCA in 2001, the same time the pen/trap definitions were expanded to include "dialing, routing, addressing, and signaling information." 18 U.S.C. § 3127.

58441 F.Supp.2d at 834-35.

59*Id.* at 835.

60396 F. Supp.2d at 765.

hide elephants in mouseholes."[61]

Lacking persuasive responses to questions such as these, the hybrid theory remains a highly implausible adventure in statutory interpretation.

. **Conclusion**

To summarize, even if the Fifth Circuit's *Historical Cell Site* holding should survive post-*Riley* challenges, nothing in that opinion undermines this court's 2005 ruling that the SCA is not an appropriate vehicle for continuous monitoring of prospective cell phone location data. The same holds true for recent decisions in other districts, like *Smartphone.* Whether or not cell site data is ultimately held worthy of Fourth Amendment protection, the Tracking Device Statute and Rule 41 of the Federal Rules of Criminal Procedure have already struck a fair balance between law enforcement and privacy concerns, and that balance is entitled to respect as the considered judgment of Congress.

Because the government's application seeks to bypass the only legitimate route Congress has mapped out for location tracking surveillance, it is denied.

Signed at Houston, Texas on July 15, 2014.

Stephen Wm. Smith
United States Magistrate Judge

61*Whitman v. Am. Trucking Ass'n*, 531 U.S. 457, 468 (2001) (refusing to find implicit in ambiguous sections of a statute an authorization that was expressly stated elsewhere).