

DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FOURTH DISTRICT
July Term 2011

SHAWN ALVIN TRACEY,
Appellant,

v.

STATE OF FLORIDA,
Appellee.

No. 4D09-3565

[September 7, 2011]

GROSS, J.

After a jury trial, Shawn Tracey was convicted of possession of more than 400 grams of cocaine, fleeing and eluding, driving while license revoked as an habitual offender, and resisting arrest without violence. We write to address his contention that the circuit court erred in denying his motion to suppress evidence derived from “real time” or prospective cell site location information (“CSLI”). We hold that there was no Fourth Amendment violation, because law enforcement used real time CSLI to track Tracey’s location only on public roads. Although there was a violation of a provision of Chapter 934, the exclusionary rule is not an authorized remedy to address the violation.

In October, 2007, Detective Jason Hendrick of the Broward County Sheriff’s Office filed an application for an order authorizing the installation and use of a pen register¹ and a trap and trace device²

¹A “pen register” is defined by Chapter 934 as “a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but such information does not include the contents of any communication.” § 934.02(20), Fla. Stat. (2009).

²A “trap and trace device” is defined by Chapter 934 as “a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but such information does not include the contents of any communication.” § 934.02(21), Fla. Stat. (2009).

regarding Tracey's cell phone.³ "Basically, a pen register is a device or process which records the telephone numbers of outgoing calls; the trap and trace device captures the telephone numbers of incoming calls." *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (Smith)*, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) (citation omitted). The application stated that Tracey was "the subject of a criminal [narcotics] investigation" and that a pen register and trap and trace device "would be an important investigative tool to record the inbound and outbound dialed digits" from Tracey's phone number, in order to "identify possible co-conspirators." This was the application's only factual allegation:

A DEA Confidential Source (CS) indicated that Shawn Alwin Tracey obtains multiple kilograms of cocaine from Broward County, for distribution on the West Coast of Florida. Furthermore, the CS contacts Shawn Tracey on the listed Metro PCS telephone number.

The application was prompted by a Drug Enforcement Administration agent who approached Hendrick with information and asked whether the two departments wished to work together in the investigation of Tracey and a cohort, Guipson Vilbon. Based on information he had received from a New York agent, the DEA agent contacted the informant, who told him that he had made trips to pick up drugs for Tracey in the past and that Tracey was currently incarcerated. The agent had no prior experience with the informant. The application for the pen register and trap device did not mention the collection of real time cell site location information.

The circuit court granted the application for a pen register and trap and trace device. In addition, although there was no request for it in the application, the order directed the cell phone company to provide the sheriff's office, "[i]n accordance" with 18 U.S.C § 2703(d), "historical Cell Site Information indicating the physical location of cell sites, along with cell site sectors, utilized for the calls" The order did not address prospective or real time CSLI. This language in the order called for the collection of a different type of information than incoming and outgoing telephone numbers. To appreciate this difference, it is necessary to have some familiarity with cell phone technology.

³The application also sought an order regarding Guipson Vilbon's cell phone; Vilbon was arrested at the same time as Tracey but was not prosecuted.

Various federal magistrates have described the technology, but we find this explanation by Judge Lenihan to be the most compact:

Cellular telephone networks divide geographic areas into many coverage areas containing towers through which the cell phones transmit and receive calls. Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the towers that serve their network and scanning for the one that provides the strongest signal/best reception. This process, called “registration”, occurs approximately every seven seconds.

As we change locations, our cell phones automatically switch cell towers. Cellular telephone companies “track the identity of the cell towers serving a phone”. When a call is received, a mobile telephone switching office (“MTSO”) gets the call and locates the user based on the nearest tower; the call is then sent to the phone via that tower. This process works in reverse when the user places a call. In urban areas, where towers have become increasingly concentrated, tracking the location of just the nearest tower itself can place the phone within approximately 200 feet. This location range can be narrowed by “tracking which 120 degree ‘face’ of the tower is receiving a cell phone’s signal.” The individual’s location is, however, most precisely determinable by triangulating the “TDOA” or “AOA” information of the three nearest cellular towers. Alternatively, the phone can be tracked extremely accurately—within as little as 50 feet—via the built-in global positioning system (“GPS”) capabilities of over 90% of cell phones currently in use. [Cellular service providers] store cell tower registration histories and other information . . . [and] now compile and retain extensive personal location information on their subscribers and the cell phones in use.

In re the Matter of the Application of the United States (Lenihan), 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (internal citations omitted), *vacated*, *In the Matter of the Application of the United States*, 620 F.3d 304 (3d Cir. 2010); *see also Smith*, 396 F. Supp. 2d at 750-51.

In December, 2007, phone calls between Tracey and an informant indicated that Tracey would be coming to Broward County to pick up drugs for transport back to the Cape Coral area, where Tracey then resided. Monitoring the location of the cell phones of Tracey and Vilbon

using real time CSLI, officers tracked Tracey's eastward trip across Florida. Tracey and Vilbon called each other ten times before Tracey arrived in Broward County. Officers set up surveillance at Vilbon's known stash houses, where the officers believed drugs were being stored. Vilbon's cell phone moved to a location near one of them. Tracey's cell phone was in almost continuous use and was tracked to the same general area. Officers determined that a GMC Envoy was from Florida's west coast; Tracey was identified as its driver. The officers were aware that Tracey's license was suspended. He was stopped and arrested for that offense. A search uncovered a kilogram brick of cocaine in the Envoy; officers stopped Vilbon and found \$23,000 in cash in his car.

Before trial in this case, Tracey moved to suppress evidence derived from real time, prospective CSLI obtained from his cell phone. He distinguished historical cell site information and explained that real time cell site information is a subset of prospective cell site information, which, he contended, requires a warrant. Tracey raised three arguments. First, officers had acquired an order to record incoming and outgoing phone numbers under "pen register and trap and trace" statutes; law enforcement exceeded the authority of the pen register order, because the detective had sought only to "record inbound and outbound dialed digits" and did not seek to track the phone's location, in either historical or real time. Second, the pen register statutes do not authorize acquisition of real time cell site information. Third, a showing of probable cause is required to acquire CSLI, and the affidavit filed in support of the pen register application did not establish probable cause.

The trial court found that (1) Tracey had standing to challenge the order and surveillance of his cell phone, but did not have standing to challenge the order and surveillance of Vilbon's cell phone; (2) the application for the order relating to his phone set forth a sufficient legal basis for the installation and use of a pen register, but did not set forth a sufficient factual basis to issue a warrant; and (3) officers had used the cell phone as a tracking device to locate Tracey behind the wheel of the vehicle:

While there was evidence that the investigators had knowledge of at least one "stash house" used by the Defendant and located within a few blocks of where he was arrested, the State was unable to establish that investigators stationed in the area stumbled upon the Defendant; rather, the evidence demonstrated that it was by using the cell phone as a tracking device that they were able to locate him

behind the wheel of a GMC Envoy at the intersection of US 441 and Miramar Parkway.

The state argued that Tracey had been seen committing a crime on a public street, which gave them an independent reason to stop him. The trial court ruled that the pen register application had not established probable cause, but that, because Tracey had been seen committing an independent crime on a public street where he had no reasonable expectation of privacy, the Fourth Amendment did not require suppression of the evidence acquired after the arrest for that independent crime. The court denied Tracey's motion to suppress.

Since it concerns the government's tracking of an individual's location on public roads, this case does not involve a Fourth Amendment violation. In *United States v. Knotts*, 460 U.S. 276 (1983), the Supreme Court confronted the government's warrantless installation of a beeper in a can of chloroform that allowed government agents to follow "an automobile on public streets and highways." *Id.* at 281. The Court held that the monitoring of beeper signals "did not invade any legitimate expectation of privacy," so that "there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment." *Id.* at 285. The Court explained:

A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the driver of the monitored vehicle] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Id. at 281-82. The Court found it significant that the monitoring of the beeper "revealed no information that could not have been obtained through visual surveillance." *United States v. Karo*, 468 U.S. 705, 707 (1984) (explaining the holding in *Knotts*). In *Mitchell v. State*, 25 So. 3d 632, 635 (Fla. 4th DCA 2009), we applied *Knotts* to hold that historical cell site information "does not implicate Fourth Amendment protections."

Here, the monitoring of the CSLI occurred only when Tracey's vehicle was on public roads, where it "could have been observed by the naked eye," so no Fourth Amendment violation occurred during Tracey's journey across Florida to Fort Lauderdale. *Karo*, 468 U.S. at 714; *see*

also *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that using a pen register on a phone did not violate the Fourth Amendment because a phone user has no reasonable expectation of privacy in the information provided to a third party by his voluntary use of a phone); *United States v. Forest*, 355 F.3d 942, 951 (6th Cir. 2004) (observing that government violated no legitimate expectation of privacy by using real time CSLI to track defendant's location, because "DEA agents could have obtained the same information by following [suspect's] car"), *vacated on other grounds*, *Garner v. United States*, 543 U.S. 1100 (2005); *United States v. Navas*, 640 F. Supp. 2d 256, 263-63 (S.D.N.Y. 2009).

We acknowledge that a compelling argument can be made that CSLI falls within a legitimate expectation of privacy. "[I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information." *In re the Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 317 (3d Cir. 2010) (emphasis in original). Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." *Id.* at 317-18 (quoting amicus brief). Location information can be "extraordinarily personal and potentially sensitive," revealing "precisely the kind of information that an individual wants and reasonably expects to be private." *Lenihan*, 534 F. Supp. 2d at 586 n.6.

Technology evolves faster than the law can keep up, extending the search capabilities of law enforcement and transforming our concept of privacy. Cell phones are ubiquitous, and some consumers embrace them as personal tracking devices. While some cell phone users share their location through geographic "tagging" on social networking platforms, others are not comfortable broadcasting their real-time location, and may maintain an expectation of privacy with respect to their location in private areas.⁴ However, on search and seizure issues, we are bound to follow United States Supreme Court precedent interpreting the Fourth Amendment. Art. I, § 12, Fla. Const. Under the current state of the law expressed in *Knotts* and *Karo*, a person's location on a public road is not subject to Fourth Amendment protection.

⁴See Adam Koppel, Note, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. Miami L. Rev. 1061, 1086-89 (2010).

Because much non-content based electronic surveillance falls outside the Fourth Amendment, most regulation of it has been by statute. “The basic contours of electronic surveillance law were fixed by the Electronic Communications Privacy Act of 1986.” (“ECPA”). *Smith*, 396 F. Supp. 2d at 751. The ECPA consists of three titles. Title I amended the 1968 federal wiretap statute;⁵ among other things, it included provisions concerning mobile tracking devices, codified at 18 U.S.C. § 3117. Title II created a new chapter of the criminal code dealing with access to stored communications and transaction records, codified at 18 U.S.C. § 2701 *et. seq.* This portion of the statute, commonly known as the Stored Communications Act (“SCA”), “authorizes government access to stored communications in the hands of third party providers.” Clifford S. Fishman & Anne T. McKenna, *Wiretapping and Eavesdropping* § 28.6 (updated June 2011). The SCA “categorizes different types of stored communications (information) and what the government must do to obtain access to those different types of information.” *Id.* Title III of the ECPA covers pen registers and trap/trace devices and is codified at 18 U.S.C. §§ 3121-27. Judge Smith has succinctly summarized “the basic architecture of electronic surveillance law erected by the ECPA”:

This statutory scheme has four broad categories, arranged from highest to lowest legal process for obtaining court approval:

- wiretaps, 18 U.S.C. §§ 2510-2522 (super-warrant);
- tracking devices, 18 U.S.C. § 3117 ([Fed.R. Crim. P.] 41 probable cause);
- stored communications and subscriber records, 18 U.S.C. § 2703(d) (specific and articulable facts);
- pen register/trap and trace, 18 U.S.C. §§ 3121-3127 (certified relevance).

Smith, 396 F. Supp. 2d at 753.

Florida has enacted statutory counterparts to the provisions of the ECPA and located them in Chapter 934, Florida Statutes (2009), entitled “Security of Communications.” Section 934.32 allows the installation of a mobile tracking device upon certification by the government that “the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.” § 934.42(2)(c), Fla. Stat. (2009). Similar to the SCA, section 934.23 allows a law enforcement officer to require a “provider of electronic

⁵Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Pub.L. No. 90-351, 82 Stat. 212 (codified at 18 U.S.C. §§ 2510-20) (the “Wiretap Act”).

communication service” to “disclose a record or other information pertaining to a subscriber of such service not including the contents of a communication,” when, among other things, the officer “[o]btains a court order for such disclosure” by offering “specific and articulable facts showing that there are reasonable grounds to believe . . . the records of other information sought are relevant and material to an ongoing criminal investigation.” §§ 934.23(4)(a)2. & (5), Fla. Stat. (2009). Mirroring Title III, sections 934.31-934.34 require a court order under section 934.33 “to install or use a pen register or a trap and trace device.” § 934.31, Fla. Stat. (2009).

Federal electronic surveillance law preempts the field under Congress’ power to regulate interstate communications. *See State v. Rivers*, 660 So. 2d 1360, 1362 (Fla. 1995). The Florida Supreme Court has written that

[t]he federal wiretap statute preempts the field of wiretapping and electronic surveillance and limits a state’s authority to legislate in this area. It allows states to adopt similar procedures authorizing state law enforcement personnel to intercept communications in a criminal investigation. Although states are free to adopt more restrictive statutes, they cannot adopt less restrictive ones.

State v. Otte, 887 So. 2d 1186, 1187-88 (Fla. 2004). Title III of the Omnibus Crime Control and Safe Streets Act of 1968 “preempted the field of the interception of wire communications.” *Rivers*, 660 So. 2d at 1362. The 1986 ECPA amended the 1968 Act and added new provisions. Congress’ intent to preempt the field of electronic surveillance as expanded by the ECPA is evident in the statutory language permitting states to access the information that is the subject of the legislation. *See* 18 U.S.C. § 3122(a)(2) (allowing a state “investigative or law enforcement officer” to make application for a pen register order to a “court of competent jurisdiction of such State,” “[u]nless prohibited by state law”); 18 U.S.C. §§ 2703(c), 2711(4) (allowing a “governmental entity” to obtain information from an electronic communication service and defining “governmental entity” as including “any State or political subdivision thereof.”).

In *Mitchell v. State*, we held that law enforcement could obtain historical CSLI, by complying with 18 U.S.C. § 2703(c), and its state counterpart, section 934.23, Florida Statutes (2009). 25 So. 3d at 634-35. We concluded that historical CSLI was “a record or other information pertaining to a subscriber or customer” of an “electronic communication

service” within the meaning of 18 U.S.C. § 2703(c) and section 934.23(4)(a). *Id.* To obtain an order for historical CSLI, law enforcement is required to “ [. . .] offer specific and articulable facts showing that there are reasonable grounds to believe the [. . .] records of other information sought are relevant and material to an ongoing criminal investigation.’ ” *Id.* at 634 (quoting § 934.23(5), Fla. Stat. (2009), which “mimics” 18 U.S.C. § 2703(d)).⁶ This is a higher standard than the “certified relevance” required for a pen register, but still less than probable cause.

Recently, the Third Circuit became the first federal court of appeal to hold that the government could obtain historical CSLI by satisfying the “specific and articulable” facts standard of 18 U.S.C. § 2703(d). *In re the Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d at 313. The court found no evidence that CSLI allows persons to be tracked precisely enough to place them at home, so there was no

⁶CSLI would seem to be obtainable under the pen register statute, were it not for another statute which excepts information, like CSLI, that can be used to identify a person’s physical location. The pen register statute, 18 U.S.C. §§ 3121-3127, authorizes the installation of a pen register and trap and trace device based on “a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation.” § 3122(b)(2). The statute defines a “pen register” as a device that records, not only the numbers dialed on a phone, but also “dialing, routing, addressing, or signaling information” transmitted by the phone, § 3127(3), which could be construed to include CSLI.

The Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001-1100, requires telecommunications carriers to ensure that their systems are available for use by law enforcement as authorized by statute. Section 1002(a)(2), which requires carriers to ensure the availability of “call-identifying information,” contains an exception:

[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)

Id. Under section 1002(a)(2), in other words, the pen register statute is not enough, by itself, to authorize the disclosure of information that could reveal a defendant’s physical location.

violation of privacy interests under *Knotts* and *Karo*. *Id.* at 312-13. The court concluded that probable cause and a warrant were not required by the Fourth Amendment in order for the government to obtain historical CSLI.⁷ *Id.*

There is some basis in federal law to support Tracey's contention that, unlike historical CSLI, an order authorizing real time CSLI requires, as a precondition, the elevated showing of probable cause, and not the lower standard of "specific and articulable facts." There is "a disagreement among courts over the standard to be applied when the government requests access to prospective or 'real time' cell site information." *In re Application of the U.S. for Orders Pursuant to Title 18 U.S.C. § 2703(d)*, 509 F. Supp. 2d 76, 78 (D. Mass. 2007); see also *In re the Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d at 310 n.6 (acknowledging the disagreement between magistrate and district court judges over the government's ability to obtain prospective CSLI). Some courts have authorized disclosure on a showing of "specific and articulable facts" under the pen register statute and section 2703.⁸ Other courts have required a showing of probable cause.⁹

⁷The Third Circuit also recognized the power of magistrates to require the government to show probable cause and obtain a warrant for CSLI. *In re the Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 319 (3d Cir. 2010). The court observed that this was a power "to be used sparingly." *Id.*

⁸ *E.g.*, *In re Application of the U.S. for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d 202 (E.D.N.Y. 2008); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 411 F. Supp. 2d 678 (W.D. La. 2006); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 433 F. Supp. 2d 804 (S.D. Tex. 2006); *Gorenstein opinion*.

⁹*E.g.*, *In re Application of the U.S. for an Order Authorizing the Use of a Pen Register*, 2009 WL 159187 (S.D.N.Y. 2009); *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re Application for an Order Authorizing the Installation and Use of a Pen Register*, 439 F. Supp. 2d 456 (D. Md. 2006); *In re Application for Pen Register & Trap & Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *In re Application of the U.S. for an Order Authorizing the Use of a Pen Register & Trap & Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005). See also *ECPA Reform and the Revolution in Location Based Tech's and Serv's: Hearing Before the Comm. on the Judiciary and Subcomm. On the Constitution, Civil Rights, and Civil Liberties*, 111th Cong. 3-4, Note 1, Exh.

We need not decide in this case whether prospective CSLI is subject to a probable cause requirement, because the state failed to meet even the less stringent standard required by section 934.23(5)—the application failed to offer “specific and articulable facts” to show that CSLI was “relevant and material to an ongoing criminal investigation.” In fact, the application did not even seek a court order for CSLI, only a pen register and a trap and trace. The application merely stated that a “Confidential Source (CS) indicated that [Tracey] obtains multiple kilograms of cocaine from Broward County for distribution on the West Coast of Florida” and that the “CS contacts” Tracey at a certain phone number. As Tracey notes in his brief, this vague language “does not explain the origin of the informant’s information; whether it was based on first-hand knowledge or was merely hearsay obtained from some other source; when [Tracey] was supposed to have last engaged in the alleged criminal conduct; when he was supposed to again engage in the alleged criminal conduct; or how the cell phone was involved in the transactions.” The statement in no way demonstrated how the confidential source was reliable. See generally *State v. Maynard*, 783 So. 2d 226, 230 (Fla. 2001); *Dozier v. State*, 766 So. 2d 1105 (Fla. 2d DCA 2000).

To say that the state violated section 943.23 in obtaining real time CSLI does not mean that an exclusionary rule applies to prevent the state from using any “evidence derived” from the violation. § 934.06, Fla. Stat. (2009). Under federal law, suppression of evidence is not a remedy for violations of the ECPA. See *United States v. Forest*, 355 F.3d at 949; *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998); *United States v. Navas*, 640 F. Supp. 2d 256, 262-63 (S.D.N.Y. 2009), *reversed on other grounds*, 597 F.3d 492 (2d Cir. 2010). “[T]he Stored Communications Act expressly rules out exclusion as a remedy; § 2708, entitled ‘Exclusivity of Remedies,’ states specifically that § 2707’s civil cause of action and § 2701(b)’s criminal penalties ‘are the *only* judicial remedies and sanctions for violations of’ the Stored Communications Act. 18 U.S.C. § 2708.” *Smith*, 155 F.3d at 1056 (emphasis in original).

Similarly, under Florida law, the exclusionary rule is not a remedy for violations of section 934.23. Section 934.28, Florida Statutes (2009) provides:

The remedies and sanctions described in ss. 934.21–934.27 are the only judicial remedies and sanctions for violation of those sections.

B (2010) (statement of Stephen Wm. Smith, U.S. Magistrate Judge), *available at* <http://judiciary.house.gov/hearings/pdf/Smith100624.pdf>.

The criminal penalties of section 934.21 and the civil remedy provided in section 934.27 are the only remedies authorized for a violation of section 934.23. Application of the exclusionary rule is not an option authorized by the statute.

For these reasons, the trial court correctly denied the motion to suppress, even though law enforcement relied on real time CSLI to locate Tracey without complying with Chapter 934. We affirm the judgments of conviction.

STEVENSON and GERBER, JJ., concur.

* * *

Appeal from the Circuit Court for the Seventeenth Judicial Circuit, Broward County; Matthew I. Destry, Judge; L.T. Case No. 07-22499CF10A.

Carey Haughwout, Public Defender, and Tatjana Ostapoff, Assistant Public Defender, West Palm Beach, for appellant.

Pamela Jo Bondi, Attorney General, Tallahassee, and Sue-Ellen Kenny, Assistant Attorney General, West Palm Beach, for appellee.

Not final until disposition of timely filed motion for rehearing.