

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Steven R. Shapiro Nathan Freed Wessler Jameel Jaffer Ben Wizner AMERICAN CIVIL LIBERTIES UNION FOUNDATION 125 Broad Street New York, NY 10004

Nancy Abudu ACLU FOUNDATION OF FLORIDA, INC. 4500 Biscayne Boulevard, Suite 340 Miami, FL 33137

Benjamin James Stevenson ACLU FOUNDATION OF FLORIDA, INC. P.O. Box 12723 Pensacola, FL 32591-2723 David Oscar Markus *Counsel of Record* MARKUS/MOSS PLLC 40 N.W. 3rd Street, Penthouse One Miami, FL 33128 (305) 379-6667 dmarkus@markuslaw.com

Jacqueline E. Shapiro 40 N.W. 3rd Street, Penthouse One Miami, FL 33128

Attorneys for Petitioner

QUESTIONS PRESENTED

In this case, as in thousands of cases each year, the government sought and obtained the cell phone location data of a private individual pursuant to

governing statute provided the prosecutor with the option to pursue a warrant but the prosecutor ignored it.

4	information collected by electronic means	
ERRE	EN BANC ELEVENTH CIRCUIT D IN HOLDING THAT THE UCT HERE WAS NOT A SEARCH 29	
A.	The Eleventh Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical &6/, « « « « « « « « « « « « «	
B.	The Eleventh Circuit Erred in Holding That Even if There Is a Reasonable Expectation of Privacy in Historical CSLI, Warrantless Search is Nonetheless 5 H D V R Q D E O H « «34 « « «	
BY AP EXCE	ELEVENTH CIRCUIT ERRED PLYING THE GOOD-FAITH PTION TO THE EXCLUSIONARY 	
CONCLUSION		
APPENDIX1a		
Opinion, United States Court of Appeals for the Eleventh Circuit(En Banc)(May 5, 2015) 1a		
• •	Inited States Court of Appeals for hth Circuit (June 11, 2014)	

*RYHUQPHQW.V \$SSOLFDWLRQ IRU 6WRUHG

TABLE OF AUTHORITIES

CASES

Arizona v. Gant,	
556 U.S. 332 (2009)	
Bond v. United States, 529 U.S. 334 (2000)	

In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information , 736 F. Supp. 2d 578 (E.D.N.Y. 2010)	
In re Application of U.S. for an Order Directing a 3 URYLGHU RI (OHF & RPPF·Q 6HUY WR 'LV 5 HFRUGV WR,53%4 K.HSuppR 2/d-5%85 (W.D. Pa. 2008)	΄ F
In re Application of U.S. for Historical Cell Site Data , 747 F. Supp. 2d 827 (S.D. Tex. 2010)	
Katz v. United States , 389 U.S. 347 (1967) 30, 32, 33	
Kyllo v. United States , 533 U.S. 27 (2001) 15, 29, 31, 32	
Minnesota v. Olson , 495 U.S. 91 (1990)	
New York v. Belton , 453 U.S. 454 (1981)	
People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009)	
Riley v. California , 134 S. Ct. 2473 (2014)passim	
Samson v. California , 547 U.S. 843 (2006)	
Smith v. Maryland , 442 U.S. 735 (1979)passim	
State v. Earls , 70 A.3d 630 (N.J. 2013)	
Stoner v. California , 376 U.S. 483 (1964)	

Tracey v. State, 152 So. 3d 504 (Fla. 2014)...... 22, 23, 28, 34 United States v. Chadwick Vernonia School Dist. 47J v. Acton , 515 U.S. 646 (1995)

OTHER AUTHORITIES

American Civil Liberties Union, Cell Phone Location Tracking Public Records Request (Mar. 25, 2013)
AT&T, Transparency Report (2015)17
Brief of Amici Curiae American Civil Liberties Union, et al., United States v. Carpenter, No. 14- 1572 (6th Cir. Mar. 9, 2015), 2015 WL 11381481 « « « « « « « « « « « « « 8 « 8 « 8 «
CTIA ² The Wireless Association, Annual Wireless Industry Survey (2014)7, 16
Daniel Solove, Conceptualizing Privacy , 90 Calif. L. Rev. 1087 (2002)
J.A. 2668 ² 3224, United States v. Graham,No. 12- W K &L U - X Q H
Orin Kerr, Eleventh Circuit Rules for the Feds on Cell-Site Records ² But Then Overreaches, Wash. Post (May 5, 2015)
Pew Research Ctr., Public Perceptions of Privacy and Security in the Post-Snowden Era (Nov. 12, 2014)
Russell M. Gold, Beyond the Judicial Fourth Am H Q G P H Q W 7 K H 3 U R V H F X W R U · V 5 R O H 47 U.C. Davis L. Rev. 1591 (2014)
Sherry F. Colb, What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 Stan. L. Rev. 119 (2002) 21
Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, Wireless Substitution: Early Release of Estimates from the

National Health Interview Survey, January ² June 2014 (Dec. 2014)16
T-Mobile, Transparency Report for 2013 & 2014 (2015) 17
Verizon Wireless, Law Enforcement Resource Team Guide (2009)
Verizon, 9 H U L] R Q · V 7 U D Qp/of65 fDrUthlel Exirist\ 5 H Half of 2015 (2015)
Will Baude, Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds , The Volokh Conspiracy (Dec. 3, 2013, 7:27 PM) 27

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

(c) Records concerning electronic communication service or remote computing service. --(1) Α governmental entity may require а provider of electronic communication service or remote computing service to disclose a record or other information subscriber pertaining to а to or customer of such service (not including the contents of communications) only when the governmental entity

> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]

(B) obtains a court order for such disclosure under subsection (d) of this section; * * *

(d) Requirements for court order. ---A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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 an d material to an ongoing criminal investigation. * * *

September 15, September 25, September 26, and October 1, 2010, in and around Miami, Florida, and DVVHUWHG WKDW WKH UHFRUGV VRXJKW ZH the investigation of those offenses. ² Pet. App. 148a. Rather than restricting the request to only the days on which the robberies occurred, however, the DSSOLFDWLRQ VRXJKW UHFRUGV IRU WKH \$XJXVW WKURXJK 2FWREHU µ D 67 days. Pet. App. 149a.

The PDJLVWUDWH MXGJH LVVXHG DQ 20 6WRUHG & HOO 6LWH ,QIRUPDWLRQµ RQ)HE Pet. App. 151a. The order directed MetroPCS, 'DYLV-V FHOOXODU VHUYLFH SURYLGHU W telephone toll records and geographic location data

FHOO VLWH μ IR Ufor' tDeYpetWodVof StukgEsQH 1 through October 6, 2010. Pet. App. 7a ²8a. MetroPCS complied, providing 183 pages of 'DYLV·V cell phone records to the government. ³ Those records VKRZ HDFK RI 'DYLV·V LQFRPLQJ DQG RXW during the 67-day period, along with the cell tower

 $FHOO VLWH\mu$ DQG GLtbdeHtoFw&/rLthRatQDO VHFWRU 'DYLV·V SKRQH FRQQHFWHG WR DW WKH VW most of the calls ZKLFK ZDV WSLFDOO\ WKH $\P > Q$

² Although none of the offenses under investigation were bank robberies, the application erroneously stated that the information sought was relevant to an investigation into offenses under the federal bank robbery statute, 18 U.S.C. § 2113. Pet. App. 148a ²149a.

³ 6 D P S O H S D J H V I U R P 'D Y L V · V U H F R U G V D U H L Q F O X G I 154a ²158a. The full records were entered as Government ([K L E L W D W W U L D O D Q G Z H U H L Q F O X G H G L Q W K appendix in the court of appeals.

DQG VWURQJH VPVet. Apple. R82, H91 a µ(quoting Trial Tr. 221, Feb. 6, 2012, ECF No. 283).

MetroPCS also produced a list of its cell sites in Florida, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. *RY·W Trial Ex. 36 . By cross-referencing the information in 'DYLV·V FDOO GHWDLO UHFRU-Site/ ZLWK 0HWU list, the government could identify the area in which 'DYLV·V SKRQH ZDV ORFDWHdeduDeQG FRXOG W 'DYLV·V ORFDM&VenReQts at multiple points each day.

2. 7 KH SUHFLVLRQ RI D FHOO SKRQH XVH reflected in FHOO VLWH ORFDWLOBSLQ µLQIRUPDWLF records depends on the size of the cell site sectors in the area. Most cell sites consist of three directional antennas that divide the cell site into three sectors, but an increasing number of towers have six sectors. Pet. App. 91a. The coverage area of cell site sectors is smaller in areas with greater density of cell towers, with urban areas having the greatest density and thus the smallest coverage areas. ⁵ Id.

The density of cell sites continues to increase as data usage from smartphones grows. Because each cell site can carry only a fixed volume of data streaming video, and other uses, as smartphone data usage increases carriers must erect additional cell sites, each covering smaller geographic areas. See CTIA ² The Wireless Association, Annual Wireless Industry Survey (2014)⁶ (showing that the number of cell sites in the United States nearly doubled from 2003 to 2013); id. (wireless data usage increased by 9,228% between 2009 and 2013). This means that in urban and dense suburban areas like Miami, many sectors cover small geographic areas and therefore can provide relatively precise information about the location of a phone. Pet. App. 91a. identifying 11,606 separate location data points (this accounts for cell site location information logged for the start and end of the calls). Pet. App. 91a. ´7 K L V averages around one location data point every five and one half minutes for those sixty-seven days, D V V X P L Q J 0 U 'D Y L V V O H S W H LdJ K W K R X U V I These records reveals a large volume of sensitive and S U L Y D W H L Q I R U P D W L R Q IoDalEidRes, W 'D Y L V - V movements, and associations:

The amount and type of data at issue revealed so much information DERXW 0 U 'D Ytd-day Mife Gth Dat most of would consider us quintessentially private. For instance, on August 13, 2010, Mr. Davis made or received 108 calls in 22 unique cell site his showing movements sectors. throughout Miami during that day. And the record reflects that many phone calls began within one cell site sector and ended in another, exposing his movements even during the course of a single phone call.

Also, by focusing on the first and last calls in a day, law enforcement could determine from the location data where Mr. Davis lived, where he slept, and whether those two locations were the same. As a government witness testified at trial ´LI \RX ORRN DW WKH majority of . . . calls over a period of time when somebody wakes up and when somebody goes to sleep, normally it is fairly simple to decipher where WKHLU KRPH WRZHU ZRXOG EH μ 7ULDC 42, Feb. 7, 2012, ECF No. 285. For example, from August 2, 2010, to \$XJXVW 0U 'DYLV·V ILUVW DQG

At trial, the government introduced the entirety of $'DYLV \cdot V \& 6/$, $LasHeFvilletado GeV * RY \cdot W$ DQG UHOLHG RQ WKHP WR HVWDEO ([location on the days of the charged robberies. A detective with the Miami-Dade Police Department WHVWLILHG WKDW 'DYLVeothion@n/earUHFRUGV SC the sites of six of the robberies. Pet. App. 11a ²12a. The detective also produced maps showing the ORFDWLRQ RI 'DYLV.V SKRQH UHODWLYH WR the robberies, which the government introduced into * R Y • W ([F. T\$h€us, evidence. Id. [t]he government relied upon the information it got from 0HWUR3&6 WR VSHFLILFDOO\ SLQ 0U 'DYLV. SDUWLFXODU VLWH LQ 0LDPTheu 3 H W \$SS prosecutor asserted to the trial judge, for example, WKDW 'OU 'DYLV.V SKRQH ≯ZuDV@ OLWHU[against the America Gas Station immediately SUHFHGLQJ DQG $D \mid W \mid U > W \mid H \mid dQ$ UREEHU\ (quoting Trial Tr. 58, Feb. 7, 2012, ECF No. 285), and DUJXHG WR WKH MXU\ LQ FORVLQJ WKDW V [Davis] literally right on top of the Advance Auto 3DUWV RQH PLQXWH EHIRUH WKDW UREEHL Trial Tr. 13, Feb. 8, 2012, ECF No. 287.

The jury convicted Davis of two counts of conspiracy to interfere with interstate commerce by threats or violence in violation of the Hobbs Act, 18 U.S.C. § 1951(a); seven Hobbs Act robbery offenses; and seven counts of using, carrying, or possessing a firearm in each robbery in violation of 18 U.S.C. § 924(c). All but the first of the § 924(c) convictions carried mandatory consecutive minimum sentences of 25 years each. As a result, the court sentenced Davis WR QHDUO\ impliseDiment (1,941)

months). ⁸ The court stated at sentencing that in light $RI 'DYLV \cdot V \setminus RXQJ DJH DQG \setminus HDUV ROG I of the offenses) and the nature of the crimes, the court believed a sentence of 40 years would have been appropriate. Sentencing Tr. 33, July 17, 2012,$

suppression motion, however, on the grounds that the government relied in good faith on the PDJLVWUDWH MXGJH·V Rthe BtoredLVVXHG XQG Communications Act, and therefore the exclusionary rule did not apply. Pet. App. 122a ²124a.

The government petitioned for rehearing en banc, and a divided Eleventh Circuit vacated the panel opinion. ¹⁰ Writing for the majority, Judge Hull held that no Fourth Amendment search occurred

privacy here, I have some concerns about the government being able to conduct 24/7 electronic tracking (live or historical) in the years to come without an appropriate judicial order.

Pet. App. 50a (internal citation omitted). Judge Jordan did not j RLQ WKH FRXUW·V FRQFOXVLRQ W is no reasonable expectation of privacy in CSLI records, but concurred that a search of CSLI is

differ in both a quantitative and a qualitative sense from other objects that might be kept on an $DUUHVWHH\cdot V SHUVRQ \mu$

This is not an isolated or occasional concern. Law enforcement is requesting staggering volumes of CSLI from service providers. In 2014, for example, points. Brief of Amici Curiae American Civil Liberties Union, et al., at 9, United States v. Carpenter, No. 14-1572 (6th Cir. Mar. 9, 2015), 2015 WL 1138148.

In Jones, Justice Alito recognized that cell phones are

requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the FRPIRUW RI WKHLU GHVNV ZH FDQ VDIHO\ dragnet-W\SH ODZ HQIRUFHPHQW SUDFWLFHV· LQ XVdH PKLV & RXUW·V LQWHUYHQWLRQ LV Q to ensure that the Fourth Amendment does not become dead letter as police accelerate their warrantless access to rich troves of sensitive personal location data.

2. This case also squarely presents the broader question of how the protections of the Fourth Amendment apply to sensitive and private data in the hands of trusted third parties.

As Justice Sotomayor noted in Jones,

it may be necessary to reconsider the premise that an individual has no reasonable expectation of phas trtT* [ont23eof 9p1(has tw631153to the ital rge, in whipeople reveal a great d@aD Zoft3lîl'ã!"\$MB £@ @ in the course of carrying out mundane tasks.

132 S. Ct. at 97 (Sotomayor, J., concuraas g). It 14.d9 not necessary in Axģn r0 = > \dot{a} Š6ã Ž M Ô£31ÔÄ4ã+C\$" Ù2ÄD\J5 Ñ2C.

pre

digital data. In Smith, this Court held that the shortterm use of a pen register to capture the telephone numbers a person dials is not a search under the Fourth Amendment. 442 U.S. at 739, 742. The Court relied heavily on the fact that when dialing a phone number, WKH FDOOHU ´YROXQWDULO\ FRQYH\>` LQIRUPDWLRQ WR WKH WHO.Oattl S444.RQH FRPSDC The Court also assessed the degree of invasiveness of the surveillance to determine whether the user had a reasonable expectation of privacy. The Court noted application of the holding of Smith, without regard for the significant changes in technology and expectations of privacy over the intervening 35 years. Pet. App. 26a ²28a. Yet three concurring judges wrote separately to register their concerns about exempting the CSLI records at issue from Fourth Amendment protections, inviting this Court to clarify the scope of the rule announced in Miller and Smith . See Pet. App. 50a ²51a (Jordan, J., concurring); id. at 58a ²59a (Rosenbaum, J., concurring).

Other courts are similarly divided. Compare In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 612 ²13 (5th Cir. 2013) \rightarrow Fifth Circuit CSLI Opinion μ (@o expectation of privacy in CSLI under Smith), with In re Application of the U.S. for an Order Directing a Provider of Elec. Comm F \cdot n Serv. W R 'L V F O R V H 5 H F R U @ V F. M R 304 W K H * R Y \cdot W 317 (3d Cir. 2010) \rightarrow Third Circuit CSLI Opinion μ @ (distinguishing Smith and holding that cell phone users may retain a reasonable expectation of privacy in CSLI).

/RZHU FRXUWV·VWUXJJOHV WR GHILQH WKH)RXUWK \$PHQGPH0com/werStot/mRsWHFWLRQV Amendment keeps pace with the rapid advance of technology.

This case presents a good vehicle for addressing application of the Fourth Amendment warrant requirement to sensitive and private records held by a third party. Without guidance from this Court, a cell phone XVHU ´FDQQRW NQRZ WKH VFR his constitutional protection, nor can a policeman NQRZ WKH VFRSH RINEW Vor® X Bekor ULW\ µ 453 U.S. 454, 459 260 (1981). As law enforcement seeks ever greater quantities of location data and other sensitive digital records, the need for this Court to speak grows daily more urgent.

Β.

expectation of privacy in historical CSLI also require protection of real-time CSLI, id. at 523. Indeed, for purposes, Fourth Amendment there is little meaningful difference between historical and realtime records, as both provide information about a pers RQ · V ORFDWLRQ LQ SULYDWH VSDFHV DQ O learn a large quantity of private information about a SHUVRQ·V DFWLmolethients.VIf DanQytobing, search of historical records is more invasive because it provides law enforcement with a completely ne w investigative power to go backward in time and track VRPHRQH·V ORFDWLRQ WKH SDVW³a verita LQ machine with no analogue in the capabilities of the founding-era constabulary

Florida law enforcement agents now must choose whether to follow the holding of Tracey and obtain a warrant before seizing CSLI, or to follow the (OHYHQWK &LUFXLW·V K &nO forgottle LQ WKLV FD warrant requirement. And even if state and local law enforcement agencies decide that Tracey articulates the controlling rule, residents of Florida will remain subject to disparate Fourth Amendment protections depending on whether they are investigated by state or federal agents. The practical protections of the Fourth Amendment should not turn on which uniform the investigators are wearing.

Likewise, a number of states require a warrant for historical CSLI by statute or under their state constitution as interpreted by the sta WH·V highest court. See Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014); Colo. Rev. Stat. § 16-3-303.5(2); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Utah Code Ann. § 77-23c-102(1)(a); 2015

(applying In re Application in the context of a suppression motion). ¹⁸

The Third Circuit takes the contrary position. In a decision issued more than a year before this & R X U W · V R SlounesLtReQThirdQCircuit held that magistrate judges have discretion to require a warrant for historical CSLI if they determine that the location information sought will implicate the VXVSHFW.V)RXUWK \$PHQGPHQW SULYDF\ showing, for example, when a person is inside a constitutionally protected space. Third Circuit CSLI Opinion, 620 F.3d at 319. In reaching that conclusion, the court rejected the argument that а FHOO SKRQH XVH Ubf b/riv/aldy/SsHelFint/ih/Dite/d/LRQ VHUYLFH SURYLGHU.V DELOLW\ WF by WKH information:

A cell phone customer has not ´YROXQWDULO\µ VKDUHG KLV ORFD information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect historical store location and LQIRUPDWLRQ 7KHUHIRUH $^{\prime}$ > Z@KHQ D

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 $DQ \setminus W K L Q J D W D O O \mu$

Id. at 317 ²18 (last alteration in original). Therefore, the court held, the third-party doctrine does not apply to historical CSLI records. Id.

3. The circuits are split over whether there is a reasonable expectation of privacy in longer-term location information collected by In United States v. Maynard, electronic means. 615 F.3d 544 (D.C. Cir. 2010), DII-G RQ RWKHU JURXQG sub nom. Jones, 132 S. Ct. 945, the D.C. Circuit held that using a GPS device to surreptitiously track a car over the course of 28 days violates reasonable expectations of privacy and is therefore a Fourth Amendment search. Id. at 563. The court explained WKDWrolonged@surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. μld. at 562. Therefore, people have a reasonable expectation of privacy in the intimate and private LQIRUPDWLRQ UHYHDOHG E\ 'SUBORQJHG *30 Id. at 563.

Although this Court affirmed on other grounds, relying on a trespass-based rationale, the

' & & L U Fax bur Wach/ under the Katz reasonableexpectation-of-privacy test remains controlling law in that circuit. ¹⁹ And that holding does not depend on the nature of the tracking technology at issue: prolonged electronic surveillance of the location of a DW SHUVRQ-V FHOO SKRQH LV OHDVW D' prolonged electronic surveillance of the location of her car. See Jones, 132 S. Ct. at 963 (Alito, J., concurring in the judgment) (explaining that law enforcement access to cell phone location information LV '>S@HUKDSV PRVW VLJQLILFDQWµ RI W GHYLFHV WKDW SHUPLW WKH PRQLWRULQJ PRYHPHQWV µ

The Eleventh Circuit rejected this reasoning RSLQHG WKDW *UHDVRQDEOH* ZKHQ LW Ηſ privacy under the Fourth Amendment do not turn on the quantity of non-content information MetroPCS FROOHFWHG LQ LWV KLVWRULFDO FHOO WRZ Pet. App. 36a. In doing so, the court of appeals widened the circuit split over whether people have a reasonable expectation of privacy in their longerterm location information ³a split that existed prior to Jones and continues today. Compare Maynard, 615 F.3d at 563 (prolonged electronic location tracking is a search under the Fourth Amendment), Pineda-Moreno, 591 F.3d 1216 ²1217 with at (prolonged electronic location tracking is not a search under the Fourth Amendment), United States v. Garcia, 474 F.3d 994, 996 299 (7th Cir. 2007) (same),

and United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010) ´\$ SHUVRQ WUDYHOLQJ YLD DXWRP public streets has no reasonable expectation of privacy in his movements from one locale to DQRWKHU µ

4. The circuits are split over whether the warrant requirement applies when there is a reasonable expectation of privacy in CSLI or other electronically collected location information. A majority of the en banc Eleventh Circuit held that, even if Petitioner had a reasonable H[SHFWDWLRQ RI SULYDF\ LQ KLV &6/, WKH warrantless seizure and search of the records was reasonable. Pet. App. 39a ²43a. That alternate holding creates a split with the courts that have

- II. THE EN BANC ELEVENTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH.
 - A. The Eleventh Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI.

The Eleventh Circuit majority held that the mere fact that the government obtained the CSLI UHFRUGV IURP 3service Vorbvirder, Hildther than from Petitioner himself, dooms his Fourth Amendment claim in light of Charleston , 532 U.S. 67, 78 (2001) $\,$ $\,$ 7 K H $\,$ U H D V R Q D E O H expectation of privacy enjoyed by the typical patient

leaving a trail of digital breadcrumbs that create a pervasive record of the most sensitive aspects of our lives. Ensuring that technological advances do not

with them virtually everywhere they go, including inside their homes and other constitutionally protected spaces, cell phone location records can reveal information about presence, location, and activity in those spaces. Pet. App. 92a, 119a ²120a. In United States v. Karo , 468 U.S. 705 (1984), this Court held that location tracking implicates Fourth Amendment privacy interests when it may reveal information about individuals in areas where they have reasonable expectations of privacy. The Court explained that using an electronic device ³there, a beeper³WR LQIHU IDFWV DERXW ´ORFDWLRQ>V YLVXDO VXUYHLOODQFH µ OLNH ZKHWKHU article is actually located at a particular time in the SULYDWH UHVLGHQFH µ RU WR ODWHU FRQIL remains on the premises, was just as unreasonable as physically searching the location without a warrant. Id. Such location tracking IDOOV ZLWKLQ WKH ambit of the Fourth Amendment when it reveals information that could not have been obtained WKURXJK YLVXDO VXUYHLOOD.QdF.Hµ IURP D S at 707; see also Kyllo, 533 U.S. at 36 (use of thermal imaging device to learn information about interior of home constitutes a search).

Second, CSLI reveals a great sum of sensitive and private i QIRUPDWLRQ DERXW D SHUVRQ-V PR and activities in public and private spaces that, at least over the longer term, violates expectations of privacy. In Jones, although the majority opinion relied on a trespass-based rationale to determine that a search had taken place, 132 S. Ct. at 949, it VSHFLILHG WKDW $^{\prime}$ > V@LWXDWLRQV LQYRO transmission of electronic signals without trespass would remain subject to Katz [reasonableexpectation-of-SULYDF\@ DIQ.D20\958.VFiµe Justices conducted a Katz analysis, and concluded that at least longer-term location tracking violates reasonable expectations of privacy. Id. at 960, 964 (Alito, J., concurring in the judgment); id. at 955 (Sotomayor, J., concurring).

This conclusion did not depend on the particular type of tracking technology at issue in Jones, and Justice Alito identified the proliferation of PRELOH GHYLFHV DV '>S@HUKDSV PRVW VLJ emerging location tracking technologies. ld. at 963. As Justice Sotomayor explained, electronic location tracking implicates the Fourth Amendment because L Wgenérates a precise, comprehensive record of a person s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations µd. at 955. This Court recently amplified that point when it explained that cell phone location data raises particularly acute SULYDF\ FRQFHUQV danHFreDcoxnSthelict LW someones specific movements down to the minute, not only around town but also within a particular building. µRiley, 134 S. Ct. at 2490 (citing Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

The records obtained by the government in this case implicate both the expectation of privacy in private spaces and the expectation of privacy in longer-term location information . They allow the government to know or infer when Davis slept at KRPH DQG ZKHQ KH GLGQ·W 3HW \$SS his movements around town, nearly down to the minute. Id. at 91a ²93a. They even allow the government to learn whom he associated with and when. SeeTrial Tr. 13, Feb. 8, 2012, ECF No. 287.

D

It is not surprising, therefore, that recent polling data shows that more than 80 percent of SHRSOH FRQVLGHU '>G@HWDLOV RI >WKHLU RYHU WLPHµ WR EH ´VHQVLWLYHµ ³evincing greater of over this information than over the contents of their text messages, a list of websites they have visited, or their relationship history. Pew Research Ctr., Public Perceptions of Privacy and Security in the Post-Snowden Era, 32, 34 (Nov. 12, 2014).²¹ Historical &6/, HQDEOHV WKH JRYHUQPHQW WR 'PRQLV our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, [which] is just the type of gradual and silent encroachment into the very details of our lives that we as a society must be YLJLODQW WRTraSedy, H152HOSOW 3 d at 522 (internal quotation marks omitted). 22

B. The Eleventh Circuit Erred in Holding That Even if There Is a Reasonable Expectation of Privacy in Historical CSLI, Warrantless Search is Nonetheless Reasonable.

²¹ http://www.pewinternet.org/files/2014/11/PI_PublicPerception sofPrivacy_111214.pdf.

²² In concluding that acquisition of historical CSLI is a Fourth Amendment search, this Court need not hold the Stored Communications Act unconstitutional. The SCA contains a mechanism for law enforcement to obtain a warrant for CSLI. See 18 U.S.C. § 2703(c)(1)(A) ´6 H F W L R Q F P D \ E H I D L U O \ F R Q V W U X H G W R S U R Y L G H I R U F Z followed Q W S U R F H G X U when the government seeks customer records that may be protected under the Fourth Amendment, including historical cell site location information. µ Fifth Circuit CSLI Opinion , 724 F.3d at 617 (Dennis, J., dissenting).

In an alternate holding, the Eleventh Circuit majority concluded that even if obtaining historical CSLI is a Fourth Amendment search, warrantless seizure and search of the records is reasonable without a warrant. Pet. App. 39a ²43a. That conclusion FRQIOLFWV ZLWK WKLV & RXUW·V OR DGPRQLWLRQ WKDW ZDUUDQP& GeHVV VHDUFK unreasonable . . . subject only to a few specifically established and well-delineated exceptions. . µCity of Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015) (quoting Arizona v. Gant , 556 U.S. 332, 338 (2009)) (alteration in original).

This Court has recognized that certain searches outside the scope of tradition4(esh11lon4(esh11lTd oa)-4(

III. THE ELEVENTH CIRCUIT ERRED BY APPLYING THE GOOD-FAITH EXCEPTION TO THE EXCLUSIONARY RULE.

The Eleventh Circuit held that, even if ZDUUDQWOHVV DFTXLVLWLRQ RI 3HWLWLRQH phone location records violated the Fourth Amendment, denial of the suppression motion would have been proper because the government relied in served by suppressing the unconstitutionally obtained evidence here.

The reasoning of Leon does not extend to the circumstances of this case for two reasons. First, the role of the judge is different. In Leon, the MXGJH·V UROH in considering a probable cause affidavit and issuing a warrant was to assess the adequacy of the factual SUREDEOH FDXVH UHFLWDWLRQ LQ WKH I declaration and to determine whether the warrant was sufficiently particularized. Those are decisions b-J 0 -1 -2(i)-4(t)-62(a)6h70(c)4(on2(r)4(c)4(umsC)4(e)-71(a)ompi)-4whenc

XQGHU WKH) RXUWKIIIShoFisHvQkGulfPH,Q4840/ μ U.S. 340, 348 ²49 (1987) (citation omitted). 3URVHFXWRUV DUH ERXQG ´WR LQWHUSUHW DQG WR ´HQIRUFH WKH ODZ ZLWKLQ FR boundaries μ 5XVVHOO BoeyonoRtoDeGJudicial) RXUWK \$PHQGPHQW 7KH,3417/BNCHFXWRU-V 5 Davis L. Rev. 1591, 1623 (2014).

Stored Communications Act makes The available to the government two relevant types of OHJDO SURFHVV D FRXUW RUGHU EDVHG JURXQGVµ WKDW WKH UHFRUGV VRXJKW DU P D W H U L D O µ LQYHVWLJDWLRQ WR DQ 2703(c)(1)(b), (d); and a probable cause warrant, id. § 2703(c)(1)(a). By the time the prosecutor applied for the SCA order in this case in February 2011, a number of magistrate judges had held that the Fourth Amendment compels the government to use the warrant mechanism under the SCA rather than casting order under § 2703(d), the an constitutionality of the latter procedure in significant doubt. See, e.g, In re Application of U.S. for Historical Cell Site Data , 747 F. Supp. 2d 827 (S.D. Tex. 2010); In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578 (E.D.N.Y. 2010), UHYG ZLWKRXW, NHb[vS 29D Q0D 0V, LinR @e Application of U.S. for an Order Directing a Provider of Elec. Comm F · Q 6 HoUD/isclose Records to the * R Y, 5784 F. Supp. 2d 585 (W.D. Pa. 2008) (opinion joined by all magistrate judges in the district) vacated and remanded for further factfinding and analysis, 620 F.3d 304 (3d Cir. 2010). The D.C. Circuit had also decided Maynard, holding that longer-term electronic location tracking is a Fourth Amendment search, 615 F.3d 544.

In light of these authorities, a cautious and responsible prosecutor should have known that seeking historical CSLI using a § 2703(d) order seriously risked violating the Constitution. The prudent course would have been to seek a warrant instead. Suppressing the evidence in this case would deter future violations by incentivizing prosecutors to choose the more constitutionally valid course when faced with a decision of what legal process to use. ²³

CONCLUSION

Jacqueline E. Shapiro 40 N.W. 3rd Street, Penthouse One Miami, FL 33128

Steven R. Shapiro