No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF TECHNOLOGY EXPERTS AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

BRIAN WILLEN
JACK MELLYN
SAMUEL DIPPO
WILSON SONSINI GOODRICH & ROSATI
1700 K Street NW
Washington, DC 20002
(202) 973-8800

ALEX ABDO
Counsel of Record
JAMEEL JAFFER
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
535 West 116th Street
314 Low Library
New York, NY 10027
(212) 854-9600
alex.abdo@knightcolumbia.org

Counsel for Amici Curiae

275003

TABLE OF CONTENTS

Page

TABLE OF CONTENTS. i

TABLE OF CITED AUTHORITIES iii

INTRODUCTION. 1

INTERESTS OF AMICI. 1

SUMMARY OF ARGUMENT 5

ARGUMENT. 6

I. CELL SITE LOCATION INFORMATION IS BECOMING INCREASINGLY DETAILED, CONTEMPORANEOUS, AND PRECISE 6

A. Cell Phones Have Become An Essential Part of American Life. 7

B. Cell Phones Constantly Generate Highly Detailed Information On Users' Locations and Movements 9

1. Law Enforcement Frequently Obtains Both Historic and Real-Time CSLI 10

C. CSLI is Routinely Collected Without User Knowledge or Consent 13

Table of Contents

Page

D. CSLI is Precise and Becoming More So Every Year 14

1. Increases in CSLI Precision Are Being Driven by Continuing Improvements in Network Architecture 14

2. The New Generation of Cell Networks Will Allow Increasingly Detailed CSLI 19

3. Carriers Are Storing Increasingly Large Amounts of CSLI and Analyzing this Data Is Increasingly Easy 22

II. CELL SITE LOCATION INFORMATION REVEALS AN EXTRAORDINARILY DETAILED PICTURE OF AN INDIVIDUAL'S LIFE, EVERY BIT AS REVEALING AS THE CONTENT OF THEIR COMMUNICATIONS 27

A. Even Discrete Pieces of CSLI Reveal Extremely Sensitive Information 27

B. Aggregated CSLI Has the Potential to Reveal Even More Sensitive Detail 32

CONCLUSION 37

TABLE OF CITED AUTHORITIES

Page

CASES

Illinois v. Lidster,
540 U.S. 419 (2004). 25

In re United States ex. rel. an Order Authorizing the Installation & Use of a Pen Register,
402 F. Supp. 2d 597 (D. Md. 2005) 10

Katz v. United States,
389 U.S. 347 (1967). 7

Riley v. California,
134 S. Ct. 2473 (2014). 8

United States v. Garcia,
474 F.3d 994 (7th Cir. 2007) 25

United States v. Graham,
824 F.3d 421 (4th Cir. 2016). 24

United States v. Jones,
565 U.S. 400 (2012). 11, 25, 32

United States v. Maynard,
615 F.3d 544 (D.C. Cir. 2010). 32

United States v. Pineda-Moreno,
617 F.3d 1120 (9th Cir. 2010). 12

Page

United States v. Stimler,
No. 15-4095, 2017 WL 3080866
(3d Cir. July 7, 2017). 16

STATUTES AND OTHER AUTHORITIES

18 U.S.C. § 2703 11

2016 Global Mobile Consumer Survey: US Edition,
Deloitte 7

Andrew Lipsman, *Mobile Matures as the Cross-Platform Era Emerges*, ComScore
(Mar. 31, 2017). 7

Bhavin Shah, *Polaris Wireless Solutions*, Law and Order Mag. (July 2013) 24

Brassil et al., *Authenticating Location with Femtocells*, Mass. Inst. Tech. 28

Brian Fung, *New FCC Proposal Would Require Pinpoint Location Accuracy for 911 Calls*, Washington Post (Feb. 20, 2014). 19

Cell Phone Location Tracking Request Response - Cell Phone Company Data Retention Chart, Am. Civil Liberties Union 22

Cellular Analysis Mapping Program v2.7, Officer.com 26

Cited Authorities

Page

Charles Blain, *Police Could Get Your Location Data Without A Warrant. That Has To End*, Wired (Feb. 2, 2017, 7:00 AM) 8

Chelsea J. Carter, *Where (and When) Do You Use Your Smartphone: Bedroom? Church?*, CNN (July 13, 2013, 9:46 PM) 7, 28

Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, Slight Paranoia Blog (Dec. 1, 2009) 12

Conference Presentation, Mahesh Patel, *Location for Public Safety and Emergency Management*, Geo Smart Asia 2016 (Oct. 18, 2016) 23

Conference Report, Arvind Thiagarajan et. al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, NSDI'11 Proc. of the 8th USENIX Conference on Networked Sys. Design and Implementation (Mar. 30, 2011) 20

Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law (Oct. 7, 2016) 18

CTIA, *Enabling the Wireless Networks of Tomorrow* 17

Data Retention in Switzerland, Digitale Gesellschaft 33

Cited Authorities

Page

Electronic Communications Privacy Act Hearing on ECPA, (Part II): Geolocation Privacy and Surveillance: *Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. and Investigations of the H. Comm. on the Judiciary*, 113 Cong. 2 (2013) . . *passim*

Enabling the Wireless Networks of Tomorrow, CTIA (Apr. 2016) 16

Events Calendar, Lutheran Church of the Reformation 31

Gavin Horn, *3GPP Femtocells: Architecture and Protocols*, Qualcomm 59 (Sept. 2010). 28

Interview by Cyrus Farivar with Malte Spitz (Jan. 4, 2011) 33

John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, Brookings (Dec. 14, 2011) 22

Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 69 (2015) 15, 20

Kai Biermann, *Betrayed by our own data*, Zeit Online (Mar. 10, 2011, 5:09 PM) 31, 34

Page

Kate Kaye, *The $24 Billion Dollar Business That Telcos Don't Want to Talk About*, Advertising Age (Oct. 26, 2015) 23

Kenneth Lipp, *AT&T is Spying on Americans for Profit*, Daily Beast (Oct. 25, 2016, 1:13 AM) 27

Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335 (2014) 24, 25

Letter from Lisa A. Judge, Principal Assistant City Att'y, Tucson Police Dep't to Dan Pochoda, Am. Civil Liberties Union (Sept. 6, 2011) . . . 11-12, 25

Mark Harris, *How Peter Thiel's Secret Company Secretive Data Company Pushed Into Policing,* Wired (Aug. 9, 2017) 26

Martha DeGrasse, *Can Verizon and AT&T Deploy 100,000 New Small Cells?*, RCR Wireless News (Oct. 29, 2015). 16

Massive Growth Projected for DAS Deployments, agl Media Group (Nov. 14, 2013). 17

Mobile Fact Sheet, Pew Research Center 7

Cited Authorities

Page

Monica Alleven, *Transit Wireless Wraps Latest Phase of Huge DAS System for NYC Subway Stations*, FierceWireless (Nov. 16, 2015, 9:55 AM) 17

Nathan Eagle et al., *Inferring friendship network structure by using mobile phone data*, 106-36 Proc. of the Nat'l Acad. of Sci. 15274, 15275 (Sept. 8, 2009).....35

Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. Times (Mar. 26, 2011) 33

Press Release, AT&T, Information for Public Safety (Sept. 30, 2017) 12

Press Release, Office of the Mass. Attorney General, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017).....30

Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, The Atlantic (Sept. 11, 2015) 9

Robinson Meyer, *No One Will Save You From Cellphone Tracking*, The Atlantic (June 2, 2016) 11

Page

Russell Brandom, *DC Prosecutors Are Ramping Up Secret Requests for Location and Internet History*, The Verge (July 19, 2017, 1:50 PM) 11

Scott Shane and Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. Times (Sept. 1, 2013) 27

Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards For Law Enforcement Access To Location Data That Congress Could Enact*, 27 Berkeley Tech. L.J. 117 (2012) 16

Tell-all Telephone, Zeit Online (March 2011) 33, 34

Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, Remarks at CTIA Super Mobility Show 2016 (Sept. 7, 2016).....17

Transparency Report, AT&T 11

Unique Features of Pen-Link v8, Pen-Link (Apr. 17, 2008).....26

Wireless Snapshot 2017, CTIA (May 2017) 8, 15

Page

Yves-Alexandre de Montjoye et al., *Predicting Personality Using Novel Mobile Phone-Based Metrics*, *in* Social Computing, Behavioral-Cultural Modeling and Prediction 48, 49 (A.M. Greenburg et al. eds, 2013) 34-35

Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Scientific Reports (Mar. 25, 2013) . . . 21, 32

INTRODUCTION

The ability of cellular phones to track their users' locations and movements has undergone a revolution since the first mobile networks were introduced in the 1980s. Originally capable only of identifying the general area from which a user was calling, today's cell site location information ("CSLI") is both rich and precise, opening the door for those with access to it, including law enforcement, to reconstruct the detailed movements, personal activities, habits, and associations of not just the direct targets of the surveillance but third parties as well. This data will only become more revealing over time as technology continues to develop to make CSLI more precise. Given the unique power of this data and its potential for misuse, amici urge the Court to hold that law enforcement officials must obtain a warrant under traditional Fourth Amendment standards before being permitted to access and use CSLI.

INTERESTS OF AMICI[1]

Amici are leading technology experts whose work addresses the privacy implications of modern communications tools. Amici have particular interest in and expertise regarding the rapid growth of CSLI technology and the serious privacy consequences that could result from its unrestrained acquisition and use by law enforcement. Amici submit this brief to explain the technology of CSLI location tracking, its rapidly

1. The parties have submitted blanket letters of consent to the filing of amicus briefs in this case. None of the parties authored this brief in whole or in part, and no one other than amici and their counsel made a monetary contribution to the preparation or submission of this brief.

increasing precision, and the ways in which it can be used to reveal highly detailed pictures of individual lives.

Ashkan Soltani is an independent researcher and technologist specializing in privacy, security, and behavioral economics. He previously served as a Senior Advisor to the U.S. Chief Technology Officer in the White House Office of Science and Technology Policy and as the Chief Technologist for the Federal Trade Commission.

Dr. Edward W. Felten is the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University, and the founding Director of Princeton's Center for Information Technology Policy. In 2015–2017 he served in the White House as Deputy U.S. Chief Technology Officer. In 2011–2012 he served as the first Chief Technologist at the U.S. Federal Trade Commission. He has published more than 150 papers in the research literature, and three books.

Dr. Matt Blaze is an associate professor of computer and information science at the University of Pennsylvania in Philadelphia, where he serves as director of the Distributed Computing Laboratory and conducts research on computer security, cryptography, network communication, and surveillance technology. In 2013, he testified before the U.S. House of Representatives on the potential privacy implications of widespread access to CSLI.

Dr. Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University. He has served as Chief Technologist of the Federal Trade Commission and as the Technology Scholar at the Privacy and Civil Liberties Board.

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the author of 14 books—including the New York Times best-seller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*—as well as hundreds of articles, essays, and academic papers.

Dr. Joseph Lorenzo Hall is the Chief Technologist and Director of the Internet Architecture project at the Center for Democracy & Technology, a Washington, DC-based non-profit advocacy organization dedicated to ensuring digital rights and that the internet remains open, innovative, and free.

Morgan Marquis-Boire is a New Zealand born security researcher and journalist. He is the Director of Security for First Look Media and a contributing writer for The Intercept.

Dr. Nicholas Weaver is a researcher focusing on security and privacy at the International Computer Science Institute in Berkeley and a lecturer in Computer Science at the University of California at Berkeley.

Dr. Stephen Checkoway is an assistant professor of computer science at the University of Illinois at Chicago where he conducts research on the security of embedded computer systems.

Dr. Dan S. Wallach is a Professor in the Departments of Computer Science and Electrical and Computer Engineering and a Rice Scholar at the Baker Institute for Public Policy at Rice University.

Adam Shostack is a consultant and the author of *Threat Modeling: Designing for Security.*

Dr. Rebecca Wright is a professor in the Computer Science Department and Director of DIMACS at Rutgers.

Dr. Carrie E. Gates is the Chief Technology Officer for an emerging Boston-based start-up focusing on providing security tools for cloud-based applications.

Scott Bradner was involved in the design, operation and use of data networks at Harvard University since the early days of the ARPANET. He retired from Harvard University in 2016 after 50 years working there in the areas of computer programming, system management, networking, IT security, and identity management.

Dr. Susan Landau is Bridge Professor in the Fletcher School of Law and Diplomacy and the School of Engineering, Department of Computer Science, Tufts University and Visiting Professor of Computer Science, University College London.

Dr. Ben Adida is the Vice-President of Engineering at Clever Inc., which specializes in securing student data in K-12 schools around the United States.

Dr. Nadia Heninger is an assistant professor in the Computer and Information Science department at the University of Pennsylvania.

Philip Zimmermann is the creator of Pretty Good Privacy, an email encryption software package, and teaches cryptography at the Delft University of Technology's Faculty of Electrical Engineering.

Dr. Sharon Goldberg is an associate professor in the Computer Science Department at Boston University. Her research focuses on practical problems in network security, and she has served on working groups of the Federal Communications Commission and the Internet Engineering Task Force.

SUMMARY OF ARGUMENT

Cell site location information is no longer confined to crude approximations, but has become increasingly sophisticated and precise. The majority of Americans now carry their phones at nearly all times, largely unaware that the devices are automatically creating a detailed and lasting record of their locations and movements. In the hands of law enforcement, these records have the potential to reveal a wide range of information about individuals' habits, activities, and associations.

The implications of unrestricted government access to CSLI for privacy and the freedoms of expression and association are profound. Even discrete pieces of CSLI can be used to uncover highly sensitive personal information—including an individual's medical conditions, religious beliefs, or political affiliations. Aggregated over time, CSLI is even more revealing, exposing an individual's social circles, romantic liaisons, and even morning and nighttime routines as they move about their house. Combined even further with publicly available data, such as maps, calendars, and social media postings, CSLI has the potential to reveal the most intimate details of a person's life.

Cellular carriers now routinely retain months and even years of CSLI data, on all of their users. And law enforcement increasingly requests large tranches of this information—making up many months—for their surveillance targets. The use of this information without adequate court supervision has the potential to profoundly unsettle legitimate expectations of privacy. Amici therefore urge the Court to treat this issue as the serious and growing challenge to individual privacy that it is, and to institute appropriate safeguards for CSLI use, including requiring law enforcement to obtain a warrant, subject to traditional Fourth Amendment standards, before obtaining or using it.

ARGUMENT

I. CELL SITE LOCATION INFORMATION IS BECOMING INCREASINGLY DETAILED, CONTEMPORANEOUS, AND PRECISE

Cellular phones have become a central part of our lives. Americans increasingly carry them everywhere, using them as a central hub for memories, work lives, and family relationships. However, these same phones broadcast a constant stream of information about their users' locations and activities—information that is frequently demanded by law enforcement and other government officials. This information—including CSLI—is far more precise and revealing now than it was in even the recent past, and will only become more so as cellular technology continues to develop.[2]

2. This brief (like the case) focuses on cell phones, but other devices that connect to cellular networks—including tablets, laptops, and wireless hotspots—could also generate CSLI records, as could any type of future technology relying on these networks.

A. Cell Phones Have Become An Essential Part of American Life

Like the wire-based telephone before it, the cellular telephone has come to play a singular and vital role in our private lives. Cf. *Katz v. United States*, 389 U.S. 347, 352 (1967) (crafting Fourth Amendment rules in recognition of "the vital role that the public telephone has come to play in private communication"). With 95% of Americans owning one, and more than 396 million units in circulation in the U.S. alone, the cell phone has become the most widely adopted piece of technology in our nation's history.[3] Americans not only use their phones, but carry them wherever they go, including home, work, school, the grocery store, their children's preschool, their doctors, churches, and more. In one study, 72% of respondents stated that they were within a five-foot reach of their phones for a majority of the time, with twelve percent even admitting to using their phones while in the shower.[4] We are also increasingly active on our phones. The average user spends nearly 3 hours per day on their phone,[5] while younger Americans report that they check their phones up to 82 times a day.[6]

---

3. *Mobile Fact Sheet*, Pew Research Center, http://www.pewinternet.org/fact-sheet/mobile/ (last visited Aug. 11, 1017).

4. Chelsea J. Carter, *Where (and When) Do You Use Your Smartphone: Bedroom? Church?*, CNN (July 13, 2013, 9:46 PM), http://www.cnn.com/2013/07/13/tech/smartphone-use-survey/.

5. Andrew Lipsman, *Mobile Matures as the Cross-Platform Era Emerges*, ComScore (Mar. 31, 2017), http://www.comscore.com/Insights/Blog/Mobile-Matures-as-the-Cross-Platform-Era-Emerges.

6. *2016 Global Mobile Consumer Survey: US Edition*, Deloitte, https://www2.deloitte.com/us/en/pages/technology-media-and-

Mobile phones have become ingrained in everyday life because of the conveniences that modern mobile technology offers. No longer just a tool that allows for increased telephone communication, smartphones have evolved into personal digital organizers, music players, cameras, email readers, and personal computers. See *Riley v. California*, 134 S. Ct. 2473, 2489 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to 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."). Cell phones have also supplanted the need for a traditional landline, with many households opting instead for cell phones carried by each family member. Owning a cell phone has become a de-facto requirement for employment of many kinds, and many people are expected, indeed required, to carry a mobile device on their person for a job.

Because of our need and desire to carry cell phones everywhere, we have also come to expect to have service everywhere. Cellular carriers have built and improved their networks to meet this growing need, placing thousands of cell sites throughout our cities, towns, office buildings, hospitals, thoroughfares, and underground subway platforms and tunnels.[7] As demand

---

telecommunications/articles/global-mobile-consumer-survey-us-edition.html (last visited Aug. 11, 2017); Charles Blain, *Police Could Get Your Location Data Without A Warrant. That Has To End*, Wired (Feb. 2, 2017, 7:00 AM), https://www.wired.com/2017/02/police-get-location-data-without-warrant-end/.

7. *Wireless Snapshot 2017*, CTIA (May 2017), https://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey.

has increased, carriers have increased the number of sites and decreased the spacing between sites. These stations allow us to communicate, work, and access information nearly anywhere in the United States. As a consequence, however, they have also allowed cellular carriers to collect increasingly fine-grained information on where we are, what we are doing, and with whom we associate. It is this second consequence—which we view as not widely understood by the public, including many cell phone users themselves—that is the focus of this amicus brief.

B. Cell Phones Constantly Generate Highly Detailed Information On Users' Locations and Movements

Cell phones and other cellular enabled devices allow users to access information about the world—but they also permit others to create a constant, lasting stream of information about those users. One of the key types of information created by our cell phones is CSLI: a record of the location of the cell user in relation to a cell tower, towers, or other cell sites within the network. CSLI is created whenever a cell phone interacts with a cell site. In its simplest version, CSLI is a running record of which cell site a cellphone interacted with, the direction of the cellphone's signal, the date and time of the signal, and, increasingly, the distance of the phone from the cell site.[8]

8. Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, The Atlantic (Sept. 11, 2015), https://www.theatlantic.com/technology/archive/2015/09/how-the-government-surveils-cellphones-a-primer/404818/.

As a tracking tool, CSLI has significant advantages over alternative location technology like GPS—including the use of the automatic interaction between the phone and base station, as well as the ability to obtain data in areas where GPS will not function because phones cannot readily receive signals from satellites, such as when underground. CSLI uses features already present in the cellular system infrastructure to pinpoint a device's location. By design, each cell phone within a specified coverage area is within radio range of at least one base station in that carrier's cellular network. Every time a cell phone interacts with a cell site, the cellular provider captures the phone's CSLI—creating a lasting data trail specific to that phone and its user.

1. Law Enforcement Frequently Obtains Both Historic and Real-Time CSLI

Cell providers routinely retain vast amounts of CSLI, and multiple types of reports can be provided or created upon request by law enforcement. These include both historical records and prospective records. Historical location information refers to records collected by the wireless service provider detailing the past location of a cell phone.[9] Prospective location information refers to all cell site information that is disclosed or generated after the government has received court permission to acquire it. This type of request also includes the generation and acquisition of real time location information through a "ping," wherein the provider sends a signal to a phone to determine its location.

---

9. See *In re United States ex. rel. an Order Authorizing the Installation & Use of a Pen Register*, 402 F. Supp. 2d 597, 599 (D. Md. 2005).

Obtaining CSLI, rather than covertly installing a GPS tracking device of the type used in *Jones*[10] (or other similar means), has become an increasingly attractive option for law enforcement to track the location of criminal suspects. AT&T received close to 60,000 requests for historical information in 2015 alone.[11] Similarly, the number of applications under 18 U.S.C. § 2703 for location or internet data (including CSLI) by the U.S. Attorney and the DOJ nearly doubled between 2015 and 2016 and increased over seven-fold between 2013 and 2016 in the Washington, D.C. area.[12] Because cell providers routinely store CSLI during the ordinary course of business, these carriers have the ability to provide law enforcement with vast amounts of data on a handset's precise location at any given time—or over an extended period of time in the past. Cell providers have become potential one-stop shops for the locations and movements of the 95% of Americans who use cell phones.

As law enforcement's appetite for CSLI has grown, the phone companies have created automated self-service websites through which government personnel can request and receive location data.[13] The availability

10. *United States v. Jones,* 565 U.S. 400 (2012).

11. Robinson Meyer, *No One Will Save You From Cellphone Tracking*, The Atlantic (June 2, 2016); see also *Transparency Report*, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (last visited Aug. 11, 2017) (most recent data).

12. Russell Brandom, *DC Prosecutors Are Ramping Up Secret Requests for Location and Internet History*, The Verge (July 19, 2017, 1:50 PM), https://www.theverge.com/2017/7/19/15998598/sealed-request-location-internet-history-ip-address-statistics.

13. Letter from Lisa A. Judge, Principal Assistant City Att'y, Tucson Police Dep't to Dan Pochoda, Am. Civil Liberties

of these automated surveillance tools has in turn led to a surge in law enforcement requests that it would have been impossible for phone company personnel to provide.[14] As Judge Kozinski notes, "When 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 comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

Union (Sept. 6, 2011), *available at* https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_tucsonpd_tucsonaz.pdf (describing the location tracking tools offered by AT&T, T-Mobile and Sprint) [hereinafter Tucson Police Dep't Letter]; see also Press Release, AT&T, Information for Public Safety (Sept. 30, 2017) *available at* https://www.al911board.com/sites/default/files/ATT%20Pinging%20and%20NCC%20Info%202013.09.30.pdf (describing AT&T's "locator tool").

14. See Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, Slight Paranoia Blog (Dec. 1, 2009), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (quoting Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, speaking on October 2009 panel at ISS World trade show: "We turned it on the web interface for law enforcement about one year ago last month, and we just passed 8 million requests. So there is no way on earth my team could have handled 8 million requests from law enforcement, just for GPS alone. So the tool has just really caught on fire with law enforcement. They also love that it is extremely inexpensive to operate and easy. . .").

C. CSLI is Routinely Collected Without User Knowledge or Consent

This information is routinely collected without the explicit knowledge—or even the active participation—of the phone's user. By design, cell phones generate a constant stream of CSLI, even when the phone is idle. Location tracking through CSLI requires only that a cell phone be on and within range of a cell site. It does not require any affirmative act on the part of the cell phone user.

This fact distinguishes cellular location tracking through CSLI from phone-based GPS tracking, which generally is available only when the phone user *intentionally* runs a location-based application on the phone, or when the target of the tracking carries another device specifically enabled for GPS. The two dominant mobile operating systems, Google's Android and Apple's iOS, explicitly notify the user and request permission before permitting an application to obtain their location information. GPS users therefore have the option of disabling their device's GPS tracking capabilities without interfering with the phone's core functionality. In contrast, the only way for a user to prevent a wireless carrier from generating CSLI records which could later be turned over to law enforcement is for the user to power off their device or put their phone in airplane mode, disabling the phone's cellular, data, and wifi services. Of course, a mobile phone without those services is no longer a mobile phone. It cannot make calls, send messages, access the internet, or be used to communicate with anyone.

D. CSLI is Precise and Becoming More So Every Year

As cellular phones have evolved from simple handsets in the 1980s to powerful handheld personal computers, the precision with which they can be tracked by the network has increased considerably. The latest generation of this technology permits the network to calculate users' locations with a precision that approaches that of GPS.[15] As cellular technology continues to improve, this trend will only accelerate, allowing anyone with access to cell site data to identify the movements of targeted individuals with ever-greater precision.

1. Increases in CSLI Precision Are Being Driven by Continuing Improvements in Network Architecture

The precision of CSLI is a product of two interrelated factors: the density of the cellular network in a given area, and the analytical capabilities of the tracking software employed by the carrier. Both of these factors have increased dramatically since the inception of cellular service in the 1980s, such that CSLI now reveals a user's location with a precision that rivals and in some cases surpasses GPS.[16]

---

15. *Electronic Communications Privacy Act Hearing on ECPA, (Part II): Geolocation Privacy and Surveillance*: *Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. and Investigations of the H. Comm. on the Judiciary*, 113 Cong. 2 (2013) (written statement of Professor Matt Blaze), https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf [hereinafter Blaze].

16. CSLI works inside buildings—which GPS does not—and thus will be able to provide much finer location information in some circumstances than GPS.

The primary factor in determining CSLI precision is the density and location of cellular base stations (sometimes called "sites" or "towers") in the user's immediate area. In a cellular network, base stations are deployed throughout the areas of service such that a cell phone will always be within radio range of at least one base station. This arrangement divides the carrier's coverage area into a mosaic of local "sectors" or "cells," each served by an antenna at a local cellular base station. When a user's phone is connected to the network, the provider can identify the sector in which the phone is located, and, in some cases, further pinpoint the phone's location within a sector.

Over time, these sectors have become much smaller, both to accommodate terrain (as in dense urban areas) and to handle the dramatically increased volume of data transmitted and received by subscribers. As cellular phones have become more popular and as users expect their devices to do more and to work in more locations, the size of the typical cell sector has been steadily shrinking. The Cellular Telecommunications Industry Association (CTIA) recently released a study finding that the number of conventional cell sites increased 57% from 2006 to 2016 (and more than 1000% since 1996).[17] And beyond that, the trend towards smaller cell sectors has been driven by the deployment of the latest generation of micro-scale cellular base stations (called, variously, "microcells", "picocells," and "femtocells").[18] A microcell services a very small

17. *Wireless Snapshot 2017*, CTIA (May 2017), https://www.ctia.org/docs/default-source/default-document-library/ctia-wireless-snapshot.pdf.

18. Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 69 (2015) [hereinafter Hoy].

area, such as the specific floor of a building or individual homes or offices.[19] The number of these small-scale cellular base stations is believed to have exceeded the number of conventional cells in the U.S. as of 2010.[20]

This trend towards an increasingly dense network composed of very small—including building- and room-sized—cells has only accelerated in recent years. Two carriers alone planned to deploy 100,000 small cells in 2016.[21] Relative to conventional cell sites, "the deployment of 100,000 small cells in only one year represents approximately one third of the total number of traditional cell sites deployed over the previous two decades."[22]

---

19. See *United States v. Stimler*, No. 15-4095, 2017 WL 3080866, at *17 (3d Cir. July 7, 2017) (Restrepo, J., concurring in part) (*quoting* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards For Law Enforcement Access To Location Data That Congress Could Enact*, 27 Berkeley Tech. L.J. 117, 132 (2012)) ("Since [2010], wireless network improvements have included the distribution of 'hundreds of thousands of 'microcells,' 'picocells,' and 'femtocells,' which function similarly to hotspots and create CSLI that 'can in some cases be more accurate than GPS.' Even the proliferation of traditional cell towers has resulted in smaller coverage areas and CSLI that is 'far more accurate—in some cases as good as GPS.'").

20. Blaze at 11.

21. Martha DeGrasse, *Can Verizon and AT&T Deploy 100,000 New Small Cells?*, RCR Wireless News (Oct. 29, 2015), http://www.rcrwireless.com/20151029/carriers/can-verizon-and-att-deploy-100000-new-small-cells-tag4.

22. *Enabling the Wireless Networks of Tomorrow*, CTIA (Apr. 2016), https://www.ctia.org/docs/default-source/default-document-library/enabling-the-wireless-networks-of-tomorrow.pdf [hereinafter CTIA, *Enabling the Wireless Networks of Tomorrow*];

Influential policy makers see small cells as a crucial part of the future of cellular telecommunications.[23]

Small cells can even be targeted towards specific public events. For example, at the 2017 Super Bowl, 783 DAS (Distributed Antenna System) antennas were placed strategically throughout the facility, potentially allowing users to be identified as sitting in a particular section of the stadium.[24] Similar systems are also increasingly being deployed to enable cell coverage on public transit routes, such as in the New York City subway system—a feature which will have the collateral effect of allowing CSLI data to identify the locations and movements of public transit customers underground.[25]

By correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations, new technology now makes it practical for a

---

see also *Massive Growth Projected for DAS Deployments*, agl Media Group (Nov. 14, 2013), http://www.aglmediagroup.com/massive-growth-in-u-s-das-deployments-projected-by-igr-research/.

23. Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, Remarks at CTIA Super Mobility Show 2016 (Sept. 7, 2016), *available at* https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0907/DOC-341138A1.pdf ("[T]here may be millions of small cell sites in the 5G future.").

24. CTIA, *Enabling the Wireless Networks of Tomorrow*, supra note 22.

25. Monica Alleven, *Transit Wireless Wraps Latest Phase of Huge DAS System for NYC Subway Stations*, FierceWireless (Nov. 16, 2015, 9:55 AM), http://www.fiercewireless.com/tech/transit-wireless-wraps-latest-phase-huge-das-system-for-nyc-subway-stations.

network operator to pinpoint a phone's latitude and longitude at a level of accuracy that can approach that of GPS.[26] The increasingly dense configuration of cells has been accompanied by a similarly sharp increase in the richness of the location-tracking data captured by cellular networks. While older-generation cellular networks from the 1980s could only identify the sector a subscriber was in, new technology allows cellular network providers to locate not just the sector in which the user's wireless device is located, but also the distance from the device to the cell site.[27]

Current commercially available versions of this "time-and-angle" location technology can pinpoint a phone's location to an accuracy of within 50 meters or less under many circumstances, and emerging versions of the technology can increase accuracy even beyond that.[28] Crucially, this can be accomplished without requiring any new or special hardware to be installed on users' phones. Users' locations can be tracked with this technology even when no calls are being made or received, as long as their phones are turned on and within a coverage area.

---

26. Blaze at 12.

27. Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law (Oct. 7, 2016), https://bol.bna.com/technology-and-shifting-privacy-expectations-perspective/ [hereinafter Silliman].

28. Blaze at 12.

2. The New Generation of Cell Networks Will Allow Increasingly Detailed CSLI

The technical improvements described above have increased the precision of CSLI to a level that would have been unimaginable even a few years ago. Today, in many circumstances, CSLI is effectively as accurate as GPS. Depending on the density of cell base stations in an area, CSLI can now often pinpoint an individual device to particular building, or even a specific room within a building.[29] This change is perhaps particularly applicable to users in urban areas, where many individual businesses, hospitals, subway systems, and other facilities have now installed dedicated micro-cells—allowing CSLI to pinpoint individuals at these locations.[30] In the past, when cell sectors were widely spaced and before the availability of the enhanced network-based location technologies now being deployed by wireless carriers, it may have been technically sound to make a distinction between location based on the cellular network (at presumably low accuracy) and that based on GPS (at higher accuracy). Today, however, this distinction is increasingly obsolete.

---

29. Blaze at 11–12.

30. To a significant degree, this increase in precision is being driven by government objectives relating to the provision of emergency services. See Brian Fung, *New FCC Proposal Would Require Pinpoint Location Accuracy for 911 Calls*, Washington Post (Feb. 20, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/02/20/new-fcc-proposal-would-require-pinpoint-location-accuracy-for-911-calls/ ("The Federal Communications Commission wants to mandate that within 30 seconds of a call, 911 dispatchers will be able to pinpoint a caller's location to within 50 meters on the correct floor. The FCC hopes that by the end of five years, 80 percent of all wireless 911 calls will benefit from the capability.").

Although CSLI precision varies based on a number of factors, its precision is highly dynamic and, at any given time, hard to predict. As individuals move around an area, the precision of CSLI data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise. This is a significant change from the introduction of cellphones in the 1980s, when CSLI could only provide an approximate location over a wide geographic area.[31]

Even imprecise CSLI can still be mined to reveal a user's location with high precision. Analytical software can track an individual as they move and reconstruct their path with a high degree of accuracy.[32] Every time an individual crosses a boundary between two cell sites, a record is created of their movement.[33] In dense urban areas or while driving, such handoffs can happen very

---

31. At trial, the government's expert, Agent Hess, testified that within a city such as Detroit, a cell site's coverage area typically would extend "a-half mile to two miles." J.A. 47. This testimony appears to refer to the maximum potential size of a cell. Today, in urban areas, cell site coverage areas are often smaller, with cell sites as close as a few hundred meters apart. Hoy at 244. Those coverage areas will almost inevitably continue to shrink as small cell sites are added to keep pace with the demands of coverage and capacity.

32. Conference Report, Arvind Thiagarajan et. al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, NSDI'11 Proc. of the 8th USENIX Conference on Networked Sys. Design and Implementation (Mar. 30, 2011), *available at* http://db.csail.mit.edu/pubs/ctrack-cr.pdf.

33. Blaze at 9–10.

frequently—often, several times per minute. If a user moves from one sector to another at a particular time, a CSLI viewer can infer that the user was on the sector boundary at that time. By superimposing the boundary onto a map, the viewer can narrow the location down further to places on the boundary on which a person is able to walk or drive. And by aggregating boundary-crossing information over time, the viewer can determine whether the user is walking or driving, and at roughly what speed, which in turn allows additional inferences regarding location (e.g., highway vs. side street vs. rail corridor).

That is not all, as a striking 2012 study demonstrated. That study, which used a data set of coarse location data from a mobile phone operator from April 2006 to June 2007, demonstrated that not only can an accurate location path be reconstructed from CSLI, but also that knowing just four *random* data points of a user's CSLI was sufficient to uniquely identify 95% of the users of the mobile phone operator.[34] In this way, CSLI can be used to effectively "fingerprint" individuals based on their patterns of movement. Given the increased precision of CSLI and other technological advances since 2012, a similar study today would only more powerfully demonstrate what can be learned from our locations and movements.

The increase in CSLI precision is the result of socially desirable progress, namely the increasing coverage, speeds, and reliability of cellular service networks.

---

34. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Scientific Reports 3 (Mar. 25, 2013), https://www.nature.com/articles/srep01376.pdf [hereinafter de Montjoye et al., *Unique in the Crowd*].

However, as discussed below, these improvements come at a high potential cost to privacy. As the Court considers this case, it should resist creating any new Fourth Amendment rule based on the assumption that the location data created by CSLI is relatively crude or minimally revealing, as it was in the 1980s. In fact, the opposite is true: CSLI has become highly revealing in the areas in which most Americans live, and will only become more so going forward.

3. Carriers Are Storing Increasingly Large Amounts of CSLI and Analyzing this Data Is Increasingly Easy

As storage costs have fallen, and as network management tools have become more sophisticated and data-intensive, cellular carriers have begun generating, storing, and retaining increasingly vast amounts of customer CSLI.[35] Even as long ago as 2011, it was estimated that "[t]he information identifying the location of each of one million people to [an accuracy of about 15 feet] at 5-minute intervals, 24 hours a day for a full year could easily be stored in 1,000 gigabytes, which would cost slightly over $50."[36] Given current trends, one can

35. See *Cell Phone Location Tracking Request Response - Cell Phone Company Data Retention Chart*, Am. Civil Liberties Union, *available at* https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Aug. 11, 2017); see also Silliman ("[O]ur network now collects more voluminous and more precise location information than [2010 and 2011]").

36. John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, Brookings 4 (Dec. 14, 2011), https://www.brookings.edu/wp-content/uploads/2016/06/1214_digital_storage_villasenor.pdf.

safely anticipate that the cost of storage will continue to fall and the amount of data stored will continue to grow in the future.

Meanwhile, retained CSLI has become increasingly useful for network management; for example, having access to historical CSLI allows cellular service providers to know which cell sites receive the most traffic, and where additional cell sites should be placed to most efficiently serve their customers.[37] Carriers have also found commercial uses for location data, allowing them to profit from the retention of data.[38] Importantly, the capability of the third-party analytical tools used by wireless carriers has rapidly improved, with newer "mass location" technology from firms such as Polaris Wireless giving carriers the ability to use historical CSLI to accurately reconstruct the locations of *all* users who were connected to their network at a given time.[39] These systems, which are marketed to carriers as ways to streamline their networks and improve their ability to respond to emergencies, have potentially significant implications for the quality and precision of historical CSLI available to

37. Blaze at 15.

38. Kate Kaye, *The $24 Billion Dollar Business That Telcos Don't Want to Talk About*, Advertising Age (Oct. 26, 2015), http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/.

39. Conference Presentation, Mahesh Patel, *Location for Public Safety and Emergency Management*, Geo Smart Asia 2016 (Oct. 18, 2016), http://geosmartasia.org/presentation/location-intelligence-for-public-safety-and-emergency-management.pdf.

law enforcement.[40] Such tools significantly amplify the accuracy of the underlying CSLI data, which, as noted above, is itself becoming more accurate over time.

Because cellular service providers retain such lengthy periods of historical CSLI data, the government is often able to request (and obtain) access to data vastly in excess of what would be provided under a traditional search warrant limited by probable cause.[41] Recent cases considered by the circuit courts have borne this out. In this case, the government obtained 127 days' worth of CSLI for Timothy Carpenter and 88 days for Timothy Sanders. Pet. App. 5a. In another recent case, the government obtained 221 days' worth (over 28,000 location data points) of CSLI for two other suspects. *United States v. Graham*, 824 F.3d 421, 446 (4th Cir. 2016) (Wynn, J. dissenting). All of that data was obtained, of course, without a warrant.

In each of these cases, had traditional methods of surveillance been utilized to collect the same amount of information, the cost to the government would have run into the hundreds of thousands of dollars for each individual surveilled.[42] For example, while foot pursuit

---

40. Bhavin Shah, *Polaris Wireless Solutions*, Law and Order Mag. (July 2013), http://www.hendonpub.com/law_and_order/articles/2013/07/polaris_wireless_location_solutions.

41. See No. 16-402 Pet. Br. 56–58, (discussing that the orders used to obtain CSLI in this case lacked particularity).

42. Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335, 350 (2014), http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones [hereinafter Bankston & Soltani].

of a subject has been estimated to cost over $30,000 for 28 days of surveillance, the same location data insight can be gathered by acquiring CSLI from cellular service providers for a tiny fraction of that cost.[43] Reconstructing a suspect's past movements over a period of months through canvass interviews and other historical sources would almost certainly have been even more expensive and time-consuming. While some carriers charge law enforcement a small fee to recoup the costs of producing CSLI reports, that fee is miniscule in comparison to the expense of traditional methods of surveillance,[44] allowing the government to conduct more invasive surveillance more indiscriminately than ever before. *Jones*, 565 U.S. at 415–416 (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004))); *Jones*, 565 U.S. at 429 (2012) (Alito, J., concurring in the judgment) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly . . . . Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."); cf. *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) ("The new technologies enable, as the old (because of expense) do not, wholesale surveillance.").

---

43. *Id.*

44. Tucson Police Dep't Letter; Bankston & Soltani at 341–350.

In addition to being relatively cheap to obtain and store, CSLI data is uniquely easy to analyze in bulk as compared to previous forms of surveillance data, such as wiretaps. Chiefly, this is because CSLI is *structured data*. That is, the information is stored in a predictable and standardized format that computers can be easily programmed to read, interpret, and even analyze, all without the need for human involvement.

A market has already developed for vendors who assist law enforcement in managing and analyzing CSLI. A number of turn-key solutions—most notably Palantir, IBM Analyst's Notebook, and Pen-Link—exist for law enforcement and other government entities to ingest cellular surveillance data directly from the wireless carriers' computer systems and convert raw CSLI data into a format suitable for easy review by investigators.[45] These analytic software tools allow anyone with CSLI

45. See *Unique Features of Pen-Link v8*, Pen-Link 4–5 (Apr. 17, 2008) ("Pen-Link offers a suite of powerful 'special' functions to help the intelligence analyst perform necessary and common analytical tasks that, when performed with traditional methods, can become tedious, error prone, and extremely time-consuming."), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1282888/09-07-14-2009-pen-link-software-sole-source.pdf (describing the capability to import 170 different data formats, used by phone companies to provide call detail records); see also *Cellular Analysis Mapping Program v2.7*, Officer.com, http://www.officer.com/product/10855725/cellular-mapping-cellular-analysis-mapping-program-v27 (last visited Aug. 11, 2017); GeoTime, https://geotime.com (last visited Aug. 11, 2017); Mark Harris, *How Peter Thiel's Secret Company Secretive Data Company Pushed Into Policing,* Wired (Aug. 9, 2017) https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/ (discussing increased use of Palantir technology by law enforcement).

to quickly and easily derive personally identifying information—including a targeted individual's movements, relationships, and private associations. Indeed, AT&T now offers a premium surveillance service to law enforcement agencies in which the company mines 26-years' worth of subscriber records, including location data, to allow agencies to look for patterns related to specific targets.[46]

II. CELL SITE LOCATION INFORMATION REVEALS AN EXTRAORDINARILY DETAILED PICTURE OF AN INDIVIDUAL'S LIFE, EVERY BIT AS REVEALING AS THE CONTENT OF THEIR COMMUNICATIONS

A. Even Discrete Pieces of CSLI Reveal Extremely Sensitive Information

As explained above, the volume, ubiquity, and structured nature of CSLI makes the privacy and expressive implications of government access to this data unique. Even a limited amount of CSLI data can be used to reveal sensitive, detailed information about individuals. This is true because of two important facts about CSLI location tracking.

---

46. See Kenneth Lipp, *AT&T is Spying on Americans for Profit*, Daily Beast (Oct. 25, 2016, 1:13 AM), http://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit (describing the extensive use of AT&T's Hemisphere system by law enforcement agencies); see also Scott Shane and Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. Times (Sept. 1, 2013) ("Some four billion call records are added to the database every day . . . ."), *available at* http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

First, most people carry their cell phone on or very near their bodies for the majority of the day, and so CSLI tracking is *personal*. In other words, any given data point of CSLI is highly likely to correspond to the precise location of an individual. This contrasts with other surveillance technologies, such as GPS devices attached to cars, which generally remain on roads, in driveways, or in garages. In contrast, the majority of individuals carry their phones on their person or within several feet the majority of the time.[47] This means that CSLI allows the government to track individuals, not just cars, and through private spaces, not just public ones. The government can collect a detailed record of the person's movements through the world, no matter how he or she chooses to travel, even recording movements through a particular building when that building contains multiple microcells.[48] In short, CSLI allows the government to track individuals not only through places where it would

47. See Chelsea J. Carter, *Where (and When) Do You Use Your Smartphone: Bedroom? Church?*, CNN (July 13, 2013, 9:46 PM), http://www.cnn.com/2013/07/13/tech/smartphone-use-survey/.

48. E.g., Brassil et al., *Authenticating Location with Femtocells*, Mass. Inst. Tech., http://web.mit.edu/ravinet/www/femto-v0.8%5B1%5D.pdf (last visited Aug. 11, 2017) ("Despite their limited wireless range (e.g., tens of meters), femtocells meet the various regulatory, compliance and spectrum use requirements of cellular base stations, including supporting location service."); Gavin Horn, *3GPP Femtocells: Architecture and Protocols*, Qualcomm 59 (Sept. 2010), https://www.qualcomm.com/media/documents/files/3gpp-femtocells-architecture-and-protocols.pdf; *Products: Femtocells*, Nokia, https://networks.nokia.com/products/femtocells (last visited Aug. 11, 2017) (describing Nokia's femtocell offering and noting that "more than 80 percent of mobile usage occurs inside buildings").

otherwise be uneconomical to do so, but even through places where it would otherwise be effectively *impossible* for the government to do so, such as within the surveillance target's own home or office.

Second, because of the increasing precision of CSLI (discussed above in Section I), even a single data point has the potential to reveal highly sensitive information about a person's associations, habits, beliefs, medical conditions, and vices. This is because of the common sense observation that individuals often go to *particular locations* for *particular purposes*. If an individual's CSLI record contains one or more data points corresponding to a certain church, the individual's religious beliefs can be inferred.[49] If an individual's CSLI record contains a data point corresponding to the time and place of a political rally or protest, the individual's political views can similarly be known or predicted.

The government could also learn, through CSLI, information and relationships generally held as confidential. Imagine, for instance, a surveillance target's CSLI data containing one or more contacts in the cell site coverage area containing the office of a prominent divorce lawyer, or a lawyer specializing in whistleblower suits. Without knowing anything about the contents of the communications of the surveillance target, the government could predict the surveillance target's personal life and protected associations.

---

49. As the ACLU noted in its brief before the Sixth Circuit, petitioner's own CSLI did in fact reveal that he attended a particular church in Detroit nearly every Sunday. See Brief of Amicus Curiae Am. Civil Liberties Union et al. at 11, 819 F.3d 880 (2016) (Nos. 14-1572 & 14-1805), *available at* https://www.aclu.org/legal-document/united-states-v-carpenter-amicus-brief.

Similarly, sensitive medical information about individuals could be determined by monitoring CSLI. Given the high and growing precision of CSLI data in urban areas, a surveillance target's CSLI could reveal with a high degree of confidence that the target visited an oncologist, a plastic surgeon, a psychiatrist, an addiction rehabilitation facility, or an abortion clinic.[50] Even a single contact in the cell site coverage areas containing one of these facilities could enable a prediction about the medical needs of the surveillance target. More frequent contacts would simply verify and increase the government's certainty about the medical condition of the target.

More revealing inferences can be drawn by combining CSLI with additional information (including public information) about the surveillance target. For instance, if the target is widely known as a mergers and acquisitions specialist and the target visits both the offices of a startup and the campus of a larger company, it could be inferred that the purchase of the startup may be in the works. If the target is a government employee and the target visits the offices of a newspaper prior to the publication of a story revealing government malfeasance, the government would similarly be able to infer the source of the story.

---

50. In one particularly striking example, advertisers sought to use mobile device location history to target pro-life messages to women who had recently visited abortion clinics—a practice that was ultimately prohibited by the Massachusetts Attorney General. See Press Release, Office of the Mass. Attorney General, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html.

Because each CSLI location data point also includes a timestamp,[51] an individual data point has the potential to convey even more detailed or nuanced information. For example, churches and community centers frequently offer different programs at different times of the day and on different days of the week. CSLI data showing that a surveillance target visited a church at 10:00 am on Sunday morning could lead to an inference of religious observance; CSLI showing that the target visited that same church at 8:30 pm on Thursday, when an Alcoholics Anonymous meeting is scheduled to take place, could lead to a very different inference.[52] The same is true of scheduled lectures at community centers or universities, movie showtimes, or political rallies.

Accordingly, it is no exaggeration to say that, by obtaining and analyzing the CSLI of an individual's cellular device, the government can gain "a clear picture of a person's habits and preferences, and indeed, of his or her life."[53] As the D.C. Circuit recognized, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular

---

51. Time is metadata that is also included with CSLI. See, e.g., J.A. 135–136.

52. E.g., *Events Calendar*, Lutheran Church of the Reformation, https://www.reformationdc.org/events-calendar (last visited Aug. 11, 2017).

53. Kai Biermann, *Betrayed By Our Own Data*, Zeit Online (Mar. 10, 2011, 5:09 PM), http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz [hereinafter Biermann].

individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 561–62 (D.C. Cir. 2010); see also *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) ("GPS monitoring generates 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."). And, as discussed in above, this information has become vastly more detailed and precise since the dawn of the cellular telephone, and will only become more so in the years to come.

B. Aggregated CSLI Has the Potential to Reveal Even More Sensitive Detail

While even a single data point of CSLI can be highly revealing of the intimate details of a person's life, the level of insight deepens when CSLI data is *aggregated*, spanning days, months, or even years.

Many, if not most, adults in the United States have a fairly consistent travel pattern on a day-to-day and week-to-week basis. As studies have recognized, the cell sites that are most often contacted by the typical user are those that serve the user's home and the user's place of employment.[54] However, when a user departs from those two cell site coverage areas, or varies their usual pattern, even more personal information about their activities can become apparent.

A striking example is provided by the case of Malte Spitz, a German politician. In 2009, Mr. Spitz sued his

54. de Montjoye et al., *Unique in the Crowd* at 4.

cellular service provider, Deutsche Telekom, to obtain the records that it kept on his cellular device, including CSLI.[55] He obtained six months of data, from August 2009 to February 2010, representing over 35,000 individual data points.[56] Mr. Spitz, *Die Zeit*, and OpenDataCity assembled the data into a nearly complete record of Mr. Spitz's life during these six months[57] As the German newspaper *Die Zeit* noted in reporting on the story and visualizing the data, "By pushing the play button, you will set off on a trip through Malte Spitz's life,"[58] including his movements, his family life, and all of his work and recreation activities. Given that the analysis of Mr. Spitz relied on 2011 tools and 2009–2010 CSLI data, a similar analysis conducted by law enforcement using the tools and data available today would inevitably be even more revealing.

As *Die Zeit*'s analysis of Mr. Spitz's CSLI noted, aggregated CSLI "reveals when Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when

---

55. Interview by Cyrus Farivar with Malte Spitz (Jan. 4, 2011), *available at* http://p.dw.com/p/10m0A; Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. Times (Mar. 26, 2011), *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html [hereinafter Cohen].

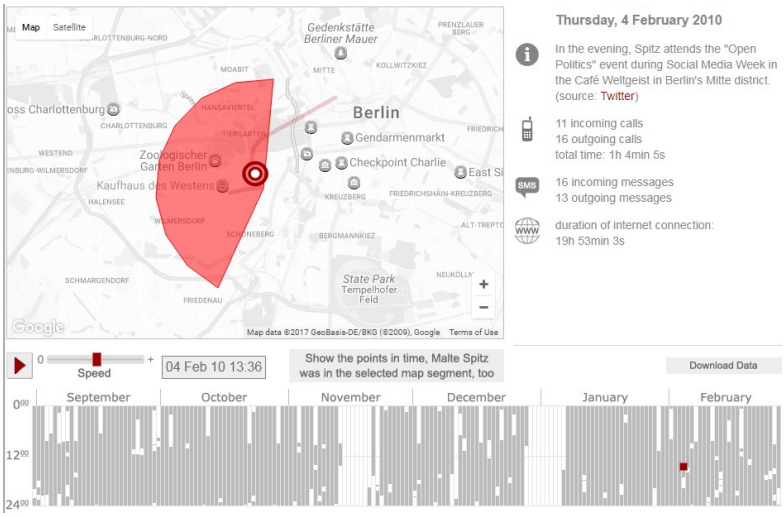
56. Cohen, supra note 55.

57. *Tell-all Telephone*, Zeit Online (Mar. 2011), http://www.zeit.de/datenschutz/malte-spitz-data-retention [hereinafter Tell-all Telephone].

58. Id.; see also *Data Retention in Switzerland*, Digitale Gesellschaft, https://www.digitale-gesellschaft.ch/vds-suisse/index_en.html (last visited Aug. 11, 2017) (similar data for the Swedish politician Balthasar Glättli).

he worked and when he slept, when he could be reached by phone and when he was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. All in all, it reveals an entire life."[59]

An interactive map provided by Die Zeit demonstrates the accuracy and richness of the CSLI data retained by Deutsche Telekom:[60]



Aggregation over time may even enable social profiling of surveillance targets. A study by researchers at MIT, Harvard, and Ecole Normale Supérieure de Lyon suggests that automated analysis of a person's CSLI records can lead to inferences about key aspects of their personality.[61]

---

59. Biermann, supra note 53.

60. *Tell-all Telephone,* supra note 57.

61. Yves-Alexandre de Montjoye et al., *Predicting Personality Using Novel Mobile*

Knowing the total distance traveled per day and the places visited by that participant, researchers could guess with statistically significant accuracy whether the participant rated low, average, or high for neuroticism, defined as their tendency to experience strong negative emotions.[62] Although research like this is undoubtedly speculative, the study provides insight into the types of inferences that may become possible when an investigator has access to the quantities of aggregated CSLI data often available to law enforcement today.

Beyond what it can reveal about an individual, aggregated CSLI data can permit the government to draw connections between people, including individuals who were not the intended target of surveillance. In one study, friendships between two individuals could be inferred with *greater than 95% accuracy* based only on how frequently those two people were co-located outside the workplace and on evenings and weekends.[63]

Once the place and purpose of a meeting has been identified through CSLI, it is trivial for other associational

---

Phone-Based Metrics, *in* Social Computing, Behavioral-Cultural Modeling and Prediction 48, 49 (A.M. Greenburg et al. eds, 2013) (ebook) *available at* https://pdfs.semanticscholar.org/6b7c/d082d71e97bb0dd8f51304e93b83b8178cc3.pdf.

62. Location information is just one type of metadata analyzed in this study that can be used to predict personality traits of individuals.

63. Nathan Eagle et al., *Inferring Friendship Network Structure by Using Mobile Phone Data*, 106-36 Proc. of the Nat'l Acad. of Sci. 15274, 15275 (Sept. 8, 2009), http://www.pnas.org/content/106/36/15274.full.pdf.

links to be drawn. For example, if law enforcement has followed the CSLI trail of a surveillance target to a Thursday, 8:30 pm Alcoholics Anonymous meeting, requesting a tower dump of the cell site serving that particular location at that particular time will reveal all the devices—and therefore individuals—in that meeting. Obtaining tower dumps of that cell site at that day and time across several weeks could permit law enforcement to uncover the repeat attendees of such a meeting. Observing whether one or more of the devices of those other repeat attendees appear in the same cell site as the surveillance target outside of the hours of the Alcoholics Anonymous meeting could permit investigators to identify persons that the target is particularly friendly with, including, for example, the target's sponsors. The same conclusions hold for other sensitive and protected associational activities—including religious evangelism, student activism, and union organizing.

* * *

The unique power—and danger—of CSLI underscores the need for care in fashioning the legal rules that govern its access. In an age of ubiquitous cell phone use, CSLI can reveal nearly everything about a person's life. Unrestricted law enforcement access to this data allows the government to reconstruct the detailed movements, personal activities, habits, relationships, and associations not just of the direct targets of its surveillance but of third parties as well. Given the sensitivity of this information and the potential for its misuse—factors that will only increase over time—the Court should make clear that the government needs to obtain a warrant before being permitted to obtain and use CSLI.

CONCLUSION

The judgment of the Court of Appeals should be reversed.

Respectfully submitted,

Alex Abdo
Counsel of Record
Jameel Jaffer
Knight First Amendment Institute
at Columbia University
535 West 116th Street
314 Low Library
New York, NY 10027
(212) 854-9600
alex.abdo@knightcolumbia.org

Brian Willen
Jack Mellyn
Samuel Dippo
Wilson Sonsini Goodrich & Rosati
1700 K Street NW
Washington, DC 20002
(202) 973-8800

Counsel for Amici Curiae