

MAINE SUPREME JUDICIAL COURT
SITTING AS THE LAW COURT

Docket No. Fra-17-12

STATE OF MAINE,
Appellee

v.

KEVIN O'DONNELL,
Appellant

On Appeal from the Franklin County Unified Criminal Docket

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION OF
MAINE, AMERICAN CIVIL LIBERTIES UNION, ELECTRONIC FRONTIER
FOUNDATION, AND MAINE ASSOCIATION OF CRIMINAL DEFENSE
LAWYERS

August 30, 2018

Zachary L. Heiden (#9476)
American Civil Liberties Union of
Maine Foundation
121 Middle Street, Suite 200
Portland, ME 04101
(207) 619-8687
Counsel for Amici Curiae

Additional Counsel Listed on Following Page

Tina Heather Nadeau,
Esq., Bar No. 4684
Executive Director
Maine Association of
Criminal Defense
Lawyers
P.O. Box 17642
Portland, ME 04112-8642

*Counsel for Amicus
Curiae Maine Association
of Criminal Defense
Lawyers*

Jennifer Lynch
Electronic Frontier
Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
Of Counsel

Nathan Freed Wessler
Jennifer Stisa Granick
Brett Max Kaufman
American Civil Liberties
Union Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500

Of Counsel

TABLE OF CONTENTS

| | |
|--|-----|
| TABLE OF AUTHORITIES | iii |
| STATEMENT OF INTEREST..... | 1 |
| STATEMENT REGARDING ORAL ARGUMENT | 2 |
| STATEMENT OF THE CASE | 3 |
| STATEMENT OF ISSUES | 4 |
| SUMMARY OF ARGUMENT..... | 5 |
| ARGUMENT..... | 8 |
| I. Cellular Service Providers Are Able To Provide Law Enforcement With Precise and Voluminous Cell Phone Location Data..... | 8 |
| II. Acquisition of Real-Time Cell Phone Location Information is a Fourth Amendment Search..... | 15 |
| A. The Third-Party Doctrine Does Not Apply to the Location Data at Issue Here..... | 15 |
| B. The Warrantless Tracking of Mr. O’Donnell’s Phone Violated His Reasonable Expectation of Privacy..... | 19 |
| 1. Real-Time Cell Phone Tracking Reveals Private Information About Presence in Protected Spaces..... | 20 |
| 2. Real-Time Cell Phone Tracking Reveals Private Information About Location and Movement Over Time..... | 23 |
| 3. Real-Time Cell Phone Tracking Provides the Government Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy..... | 25 |
| C. The Warrantless Tracking of Mr. O’Donnell’s Phone Interfered with the Security of His Person, Papers, and Effects..... | 28 |
| D. In the Absence of Exigent Circumstances, Real-Time Cell Phone Location Tracking Requires a Warrant..... | 33 |
| III. The Legislature Intended to Provide a Suppression Remedy for Violations of 16 M.R.S. § 648..... | 35 |
| CONCLUSION..... | 40 |
| CERTIFICATE OF SERVICE..... | 42 |
| CERTIFICATE OF SIGNATURE | 43 |

TABLE OF AUTHORITIES

Cases

| | |
|---|----------------|
| <i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018) | passim |
| <i>Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.</i> , 511 U.S. 164 (1994)..... | 38 |
| <i>Collins v. Virginia</i> , 138 S. Ct. 1663 (2018) | 29 |
| <i>Commonwealth v. Almonor</i> , No. 1283CR00492 (Plymouth Sup. Ct. Sept. 8, 2016), <i>appeal pending</i> , No. SJC-12499 (Mass.) | 20 |
| <i>Conroy v. Aniskoff</i> , 507 U.S. 511 (1993)..... | 39 |
| <i>Florida v. Jardines</i> , 569 U.S. 1 (2013)..... | 29 |
| <i>Ford Motor Co. v. Darling’s</i> , 2016 ME 171 | 35 |
| <i>Grady v. North Carolina</i> , 135 S. Ct. 1368 (2015)..... | 29, 30 |
| <i>Hickson v. Vescom Corp.</i> , 2014 ME 27 | 36 |
| <i>In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.</i> , 396 F. Supp. 2d 747 (S.D. Tex. 2005)..... | 33 |
| <i>In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.</i> , 849 F. Supp. 2d 526 (D. Md. 2011)..... | 12, 16, 17, 20 |
| <i>In re Application of U.S. for Historical Cell Site Data</i> , 724 F.3d 600 (5th Cir. 2013)..... | 17, 31 |
| <i>Kyllo v. United States</i> , 533 U.S. 27 (2001)..... | 6, 21, 22, 25 |
| <i>Mahaney v. Miller’s, Inc.</i> , 669 A.2d 165 (Me. 1995)..... | 38 |
| <i>Maine Today Media, Inc. v. State</i> , 2013 ME 100 | 36 |
| <i>McPheters v. Page</i> , 83 Me. 234, 22 A. 101 (1891) | 31 |

| | |
|---|------------|
| <i>Milner v. Dep't of Navy</i> , 562 U.S. 562 (2011)..... | 39 |
| <i>People v. Weaver</i> , 909 N.E.2d 1195 (N.Y. 2009) | 24 |
| <i>Prince Jones v. United States</i> , 168 A.3d 703 (D.C. 2017) | 27, 28 |
| <i>Rakas v. Illinois</i> , 439 U.S. 128 (1978)..... | 31 |
| <i>Riley v. California</i> , 134 S. Ct. 2473 (2014) | 20, 26, 30 |
| <i>See v. City of Seattle</i> , 387 U.S. 541 (1967)..... | 21 |
| <i>Silverman v. United States</i> , 365 U.S. 505 (1961) | 31 |
| <i>Skinner v. Ry. Labor Executives' Ass'n</i> , 489 U.S. 602 (1989) | 17 |
| <i>Smith v. Maryland</i> , 442 U.S. 735 (1979) | 18 |
| <i>State v. Andrews</i> , 134 A.3d 324 (Md. Ct. Spec. App. 2016) | 22 |
| <i>State v. Earls</i> , 70 A.3d 630 (N.J. 2013) | 20, 22 |
| <i>State v. Hutchinson</i> , 2009 ME 44 | 15 |
| <i>State v. Oken</i> , 569 A.2d 1218 (Me. 1990) | 22, 33 |
| <i>Stone v. Bd. of Registration in Med.</i> , 503 A.2d 222 (Me. 1986) | 39 |
| <i>Stoner v. California</i> , 376 U.S. 483 (1964)..... | 21, 22 |
| <i>Tracey v. State</i> , 152 So. 3d 504 (Fla. 2014)..... | passim |
| <i>United States v. Jones</i> , 565 U.S. 400 (2012) | passim |
| <i>United States v. Karo</i> , 468 U.S. 705 (1984) | 21 |
| <i>United States v. Lambis</i> , 197 F. Supp. 3d 606 (S.D.N.Y. 2016) | 22 |
| <i>United States v. Miller</i> , 425 U.S. 435 (1976) | 18 |
| <i>United States v. Pineda-Moreno</i> , 617 F.3d 1120 (9th Cir. 2010)..... | 10 |

United States v. Powell, 943 F. Supp. 2d 759 (E.D. Mich. 2013).....19

United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).....27

Rules & Statutes

12 R.I. Gen. Laws § 12-32-2.....32

12 R.I. Gen. Laws § 12-32-3.....38

16 M.R.S. § 64735

16 M.R.S. § 648 passim

16 M.R.S. § 6504

16 M.R.S. § 650-A 8, 37, 38, 40

18 U.S.C. § 1039 33, 38

18 U.S.C. § 312732

47 U.S.C. § 100232

47 U.S.C. § 22233

725 Ill. Comp. Stat. 168/10.....32

Cal. Penal Code § 1546.132

Ind. Code § 35-33-5-12.....32

Kan. Stat. Ann. § 22-250232

M.R.S. § 65036

M.R.U. Crim. P. 41B37

Md. Code Ann. Crim. Proc. § 1-203.1.....32

Me. Const. art. IV, pt. 3, § 239

| | |
|-------------------------------------|----|
| Minn. Stat. § 626A.42..... | 32 |
| Mont. Code Ann. § 46-5-110..... | 32 |
| N.H. Rev. Stat. Ann. § 644-A:2..... | 32 |
| Utah Code Ann. § 77-23c-102..... | 32 |
| Vt. Stat. Ann. tit. 13, § 8102..... | 32 |

Other Authorities

| | |
|--|-------|
| David Schneider, <i>New Indoor Navigation Technologies Work Where GPS Can't</i> , IEEE Spectrum (Nov. 20, 2013)..... | 9 |
| <i>E911 Compliance FAQs</i> , Verizon Wireless..... | 10 |
| Fed. Bureau of Investigation, <i>Domestic Investigations and Operations Guide</i> § 18.6.8.4.2.5.3 (2011)..... | 7, 34 |
| <i>In re Wireless E911 Location Accuracy Requirements</i> , PS Docket No. 07-114, Fourth Report and Order (F.C.C. Jan. 29, 2015)..... | 9 |
| Jamesa J. Drake, <i>Reviving Maine's State Constitutional Protection Against Unreasonable Searches and Seizures</i> , 68 Me. L. Rev. 321 (2016)..... | 15 |
| Jari Syrjärinne & Lauri Wirola, <i>Quantifying the Performance of Navigation Systems and Standards for Assisted-GNSS</i> , InsideGNSS (Sept./Oct. 2008)..... | 11 |
| Matt Blaze, <i>How Law Enforcement Tracks Cellular Phones</i> , Exhaustive Search (Dec. 13, 2013)..... | 10 |
| <i>Mobile Fact Sheet</i> , Pew Research Center (Feb. 5, 2018)..... | 14 |
| Report and Order and Further Notice of Proposed Rulemaking, <i>In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.</i> , 11 FCC Rcd. 18676 (1996)..... | 9 |
| Sprint, <i>Sprint Corp. Transparency Report</i> (2018)..... | 14 |

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).....12

The Electronic Communications Privacy Act (ECPA), Part 2:
Geolocation Privacy & Surveillance: Hearing Before the
Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations
of the H. Comm. on the Judiciary 113th Cong. (2013) 11, 12

T-Mobile US, Inc., *Transparency Report for 2017* (2018)14

Verizon, *United States Report*14

What is GPS?, Garmin11

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION OF MAINE, AMERICAN CIVIL LIBERTIES UNION, ELECTRONIC FRONTIER FOUNDATION, AND MAINE ASSOCIATION OF CRIMINAL DEFENSE LAYWERS

STATEMENT OF INTEREST

The American Civil Liberties Union (“ACLU”) is a nationwide, non-profit, non-partisan organization of nearly two million members dedicated to defending the civil liberties and civil rights guaranteed by the Constitution. The American Civil Liberties Union of Maine (“ACLU of Maine”), founded in 1968, is the Maine state affiliate of the ACLU. The ACLU and ACLU of Maine have a long history of involvement, both as direct counsel and as amicus curiae, in cases involving the protection of rights under the Fourth Amendment to the U.S. Constitution and article 1, section 5 of the Maine Constitution, including ensuring that those rights remain robust in the face of evolving technology. The ACLU was counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the case that prompted this Court’s call for amicus briefing here.

The Electronic Frontier Foundation (“EFF”) is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for nearly 30 years. With more than 40,000 active donors, including donors in Maine, EFF represents technology users’ interests in court cases and broader policy debates. EFF served as amicus in numerous cases addressing Fourth Amendment protections for cell phone location

information, including *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016); and *State v. Andrews*, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

The Maine Association of Criminal Defense Lawyers is a statewide organization of criminal defense attorneys dedicated to the fair administration of criminal justice throughout the State of Maine and the defense of all people accused of crimes. MACDL has an interest in the present case, as its facts and issues are likely to arise in future cases impacting our member attorneys and their clients.

STATEMENT REGARDING ORAL ARGUMENT

The Court held oral argument in this case on October 12, 2017, prior to the U.S. Supreme Court's decision in *Carpenter v. United States*. Amici respectfully submit that, in light of the Supreme Court's clarification of Fourth Amendment doctrine, additional oral argument would aid this Court in its decision in this case. Should the Court decide to schedule additional argument, Amici respectfully seek

leave to participate. Nathan Freed Wessler, undersigned attorney for amicus ACLU, who argued *Carpenter* for the defendant-appellant before the Supreme Court, and who has argued a number of cases involving cell phone location tracking in state and federal appellate courts, would be pleased to participate in oral argument with leave of the Court.

STATEMENT OF THE CASE

While investigating a burglary of an unoccupied home in 2015 in which Defendant–Appellant Kevin O’Donnell and a second individual, Danielle Nelson, were suspects, Sergeant Jared Austin of the Ranglely Police Department directed a dispatcher to submit emergency requests to Verizon to track and locate O’Donnell’s and Nelson’s cell phones in real time. (A. 60–61.) Police did not obtain a search warrant or other judicial authorization before submitting the requests. Sgt. Austin testified that Verizon assisted law enforcement by “ping[ing]” O’Donnell’s and Nelson’s phones, and transmitting their cell phone location data back to him. (A. 65.) The location data “showed both cell phones in close proximity to one another . . . and [that] they were both in close proximity to two separate motels” in Lewiston. (A. 65.) Working with Sgt. Austin, Lewiston police searched the area indicated by the cell phone location data, and located O’Donnell and Nelson at a Motel 6 in Lewiston. (A. 97–102.)

Mr. O’Donnell filed a motion to suppress, arguing that the warrantless tracking of his cell phone violated his rights under the Fourth Amendment, the Maine Constitution, and state and federal statutes. (A. 122–23.) The trial court agreed with Mr. O’Donnell that there were no exigent circumstances that would justify dispensing with the warrant requirement imposed by state law, 16 M.R.S. §§ 648, 650(4). (A. 26.) (The State does not contest this conclusion on appeal. (State’s Br. 10.)) The court denied suppression, however, on the grounds that “the warrantless acquisition of cell phone location information from a third-party service provider does not constitute a search within the meaning of the Fourth Amendment,” (A. 24), and that the legislature did not intend to create a suppression remedy for violations of the state statute requiring a warrant for cell phone location data, (A. 29).

STATEMENT OF ISSUES

- 1) Whether law enforcement’s acquisition of a person’s real-time cell phone location information from that person’s cellular service provider is a search under the Fourth Amendment and article 1, section 5 of the Maine Constitution.
- 2) Whether the proper remedy for violation of 16 M.R.S. § 648, which requires a warrant for law enforcement access to a person’s cell phone location information in the absence of a qualifying emergency, is

suppression of evidence derived from the illegally obtained location information.

SUMMARY OF ARGUMENT

For the 95 percent of Americans who own cell phones, the technology has become “such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society.” *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (quotation marks and citation omitted). In this case, as in thousands each year, the government sought to exploit this essential technology by requesting that a suspect’s cellular service provider track and locate the phone in real time. Service providers can typically comply with such requests by sending a signal to the phone that surreptitiously enables its GPS chip and obtains the phone’s precise coordinates. Because people carry their phones with them virtually everywhere they go, this capability effectively gives the government the power to instantaneously install a tracking beacon on any person at any time. Unless constrained by the Fourth Amendment and article 1, section 5 of the Maine Constitution, that capability poses a grave threat to privacy and constitutes a sweeping expansion of government power.

In *Carpenter*, the Supreme Court held that the government’s warrantless acquisition of a person’s historical cell phone location records infringes on reasonable expectations of privacy under the Fourth Amendment. In doing so, the

Court rejected the government's claim that the mere fact that the records are held by the cellular service provider vitiates the cell phone user's privacy interest under the Fourth Amendment. Rather, because of the high sensitivity of cell phone location data and the unavoidability of its creation, the Fourth Amendment's protections apply. That rule applies squarely to the cell phone location data in this case.

Moreover, as with the historical cell phone location records at issue in *Carpenter*, there is a reasonable expectation of privacy in the real-time cell phone tracking data in this case. Tracking a phone in real time can reveal a wealth of information about patterns of activity that lays bare "familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S. Ct. at 2217 (citation omitted). Because of the precision of the data, it can also reveal location in homes, offices, hotel rooms, and other spaces that receive the highest protection under the Fourth Amendment, and for which warrantless searches using both traditional and technological means are forbidden. *See Kyllo v. United States*, 533 U.S. 27, 40 (2001). At bottom, real-time cell phone tracking threatens to undermine the "degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter*, 138 S. Ct. at 2214, because it gives police a capability unimaginable before the cell phone age—the power to pluck a person's precise location out of thin air. In order to prevent this capability from feeding a

“too permeating police surveillance,” *id.* at 2214, the Fourth Amendment’s warrant requirement applies. Of course, when law enforcement agents have probable cause but exigent circumstances prevent them from applying for a warrant, they may proceed without one. *Id.* at 2222–23. But in a case like this, where no such exigency existed, a warrant is required. That has been the rule followed by the Federal Bureau of Investigation for years,¹ and this Court should make clear to Maine law enforcement that the Fourth Amendment requires it in state investigations as well.

Alternately, real-time cell phone location tracking is a search because it interferes with an individual’s control over his or her person, papers, and effects within the meaning of the Fourth Amendment. By forcing a person’s cell phone to transmit its coordinates, the government reduces that person to a trackable object, converts the person’s cell phone into an active tracking device, and misappropriates the person’s location data without consent. Because this tracking is incompatible with people’s rights to control use of their persons, papers, and effects—i.e., their property rights—it constitutes a Fourth Amendment search. *See Carpenter*, 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting); *United States v. Jones*, 565 U.S. 400, 405 (2012).

¹ *See* Fed. Bureau of Investigation, *Domestic Investigations and Operations Guide* § 18.6.8.4.2.5.3, at 18-113–14 (2011), *available at* <https://theintercept.com/document/2017/01/31/domestic-investigations-and-operations-guide>.

Finally, suppression is independently justified in this case because the government violated Maine's statutory requirement that, absent a qualifying emergency, police can track a person's cell phone only with a valid warrant. 16 M.R.S. § 648. The Superior Court erred in relying on equivocal legislative history to conclude that there was no suppression remedy for violations of the statute. To the contrary, the plain language of the statute provides that location information and evidence derived from it may be used at trial only if a copy of the warrant is furnished to the defense in advance. 16 M.R.S. § 650-A(1). Because the government chose not to obtain a warrant in this case, it necessarily failed to comply with this requirement and therefore was not entitled to the introduction of information derived from the cell phone tracking.

ARGUMENT

I. Cellular Service Providers Are Able To Provide Law Enforcement With Precise and Voluminous Cell Phone Location Data.

Because of capabilities built into cell phone networks and handsets in response to federal regulatory requirements, cellular service providers are able to locate cell phones—and by extension the phones' users—upon law enforcement's request. They can do so with enough precision to place a person within a specific room of a home, even if they have no idea in advance who that person is or where they might be located.

This capability stems from rules first adopted in 1996 and fully implemented by 2001, under which the Federal Communications Commission (FCC) required cellular service providers to have “the capability to identify the latitude and longitude of a mobile unit making a 911 call.”² The precision and accuracy of this mandated cell phone location capability is increasing. The FCC has adopted rules to increase law enforcement’s ability to locate callers when they are indoors,³ and to require service providers to develop techniques to determine the altitude of the phone, and thus on which floor of a building it is located.⁴

Although this capability was initially developed to assist in responding to 911 calls, service providers now provide the same cell phone location information to law enforcement pursuant to investigative requests. Rather than wait for the customer to initiate an emergency call, the service provider is able to connect to the customer’s phone and thereby determine its location. That is, law enforcement can ask a wireless carrier to generate new, precise, real-time location data by acquiring information from the target’s phone. This can be done “on demand or at periodic

² Report and Order and Further Notice of Proposed Rulemaking, *In re Revision of the Comm’n’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.*, 11 FCC Rcd. 18676, 18683–84 (1996).

³ *In re Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Fourth Report and Order at 1 (F.C.C. Jan. 29, 2015) (“Wireless E911 Order”), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf; David Schneider, *New Indoor Navigation Technologies Work Where GPS Can’t*, IEEE Spectrum (Nov. 20, 2013), <http://spectrum.ieee.org/telecom/wireless/new-indoor-navigation-technologies-work-where-gps-cant>.

⁴ Wireless E911 Order at 3-4.

intervals.”⁵ As occurred in this case, some providers send location data to law enforcement via email or similar means, (*see* A. 65), while other providers allow law enforcement “direct access to users’ location data” by logging into an “automated . . . web interface” provided by the carrier. *United States v. Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc).

The ability to locate and track a phone in real time has no relationship to whether the phone is actually in use. As long as a phone is connected to the network, service providers can engage their location-tracking capabilities to find it at the request of law enforcement—a user cannot disable this functionality without turning the phone off or putting it into airplane mode (which, of course, renders the phone useless as a phone).⁶ Even disabling the location services setting on a smart phone cannot stop the carrier from determining the phone’s precise location in real time: while the location privacy setting prevents third-party applications (“apps,” like Google Maps) from accessing the phone’s location information, it does not impact the carrier’s ability to locate the device.

Service providers can obtain the real-time location of a cell phone upon law enforcement request in at least two ways, depending on the structure of the

⁵ Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, Exhaustive Search (Dec. 13, 2013), <http://www.mattblaze.org/blog/celltapping/>.

⁶ *E.g.* *E911 Compliance FAQs*, Verizon Wireless, <http://www.verizonwireless.com/support/e911-compliance-faqs>.

carrier's network: (1) by using hardware built into the phone ("handset-based" technology); and/or (2) by analyzing the phone's interactions with the network's base stations, or "cell sites" ("network-based" technology).⁷

Handset-based technology uses a mobile device's "special hardware that receives signals from a constellation of global positioning satellites."⁸ The Global Positioning System ("GPS") chip installed in a cellular telephone uses radio signals from GPS satellites orbiting Earth to calculate its own location within 10 meters.⁹ Newer receivers, with enhanced communication to ground-based technologies that correct signal errors, can identify location within three meters or closer, and have a vertical accuracy of five meters or better 95 percent of the time.¹⁰

Service providers do not typically maintain GPS coordinate records for phones using their networks, but, upon law enforcement request, they can remotely activate a phone's GPS functionality and then cause the phone to transmit its

⁷ The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy & Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary 113th Cong. 6 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ("Blaze Hearing Statement"), *available at* http://judiciary.house.gov/_files/hearings/113th/04252013/Blaze%2004252013.pdf.

⁸ *Id.* at 7; *see also* Wireless E911 Order at 5 n.11.

⁹ Blaze Hearing Statement at 7; *see also In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.* (hereinafter "*Maryland Real-Time Order*"), 849 F. Supp. 2d 526, 540–41 (D. Md. 2011) (noting that GPS -derived cell phone location data can be precise enough to locate a cell phone within a residence).

¹⁰ This is sometimes referred to as Assisted GPS or A-GPS. Jari Syrjärinne & Lauri Wirola, *Quantifying the Performance of Navigation Systems and Standards for Assisted-GNSS*, InsideGNSS (Sept./Oct. 2008), <http://insidegnss.com/wp-content/uploads/2018/01/sepoct08-gnssolutions.pdf>; *What is GPS?*, Garmin, <http://www8.garmin.com/aboutGPS/>.

coordinates back to the provider. *Maryland Real-Time Order*, 849 F. Supp. 2d at 534. Providers can “ping” phones “unobtrusively, i.e., without disclosing to a telephone user the existence either of the Carrier’s signal requesting the telephone to send a current GPS reading or that telephone’s response.” *Id.* at 531 (citing government application).

Service providers may also precisely locate a phone using network-based calculations. Network-based technologies use existing cell site infrastructure to identify and track location by silently “pinging” the phone and then triangulating its precise location based on which cell sites receive the reply transmissions.¹¹

Service providers can obtain this cell site location information even when no call is in process, and can locate a phone with GPS-level accuracy. *Maryland Real-Time Order*, 849 F. Supp. 2d at 534.

In addition to these capabilities for precisely locating cell phones in real time at law enforcement request, service providers also routinely log and retain information about the location of cell phones as they interact with the network. Thus, even in cases where law enforcement is unable to obtain real-time location information from the service provider, it will generally be able to obtain “historical” location data that is generated and saved on an ongoing basis, and that

¹¹ Blaze Hearing Statement at 12; 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, 128 (2012).

can reflect the phone's location as recently as a few seconds or minutes ago, and as far back in time as five years. *See Carpenter*, 138 S. Ct. at 2218. "Each time the phone connects to a cell site," whether to make or receive a phone call, send or receive a text message, make a data connection, or merely register with the network so that it can receive calls, "it generates a time-stamped record known as cell-site location information (CSLI)." *Id.* at 2211–12. CSLI records (also known as "historical CSLI," to distinguish them from real-time data) generally identify the cell site (i.e., cell tower) and the directional antenna of that tower that the phone was connected to at any given time. As the Supreme Court has explained, "[t]he precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas." *Id.* Although in the past CSLI was often less precise than real-time GPS data, advances in technology, including the proliferation of "small cells" with broadcast radii as small as a few rooms in a house, as well as "new technology measuring the time and angle of signals hitting [providers'] towers," mean that "the accuracy of CSLI is rapidly approaching GPS-level precision." *Id.* at 2219.

The power to track and locate any person’s cell phone affects virtually all Mainers. Ninety-five percent of Americans now own cell phones,¹² and most carry them with them everywhere they go. As the Supreme Court has explained, without constitutional regulation, this power will give the government the unfettered ability to “achieve[] near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” *Carpenter*, 138 S. Ct. at 2218. Indeed, across the nation, the government invokes this power with frequency. Sprint and T-Mobile, for example, respectively received 59,762 and 46,395 real-time cell phone location requests from law enforcement in 2017.¹³ Verizon, Mr. O’Donnell’s provider, received 21,863 requests for location data (including historical and real-time data) in the first half of 2018, and 31,239 warrantless emergency requests for information from law enforcement (some but not all of which sought location data) in the same period.¹⁴

¹² *Mobile Fact Sheet*, Pew Research Center (Feb. 5, 2018), <http://www.pewinternet.org/fact-sheet/mobile/>; *see also Carpenter*, 138 S. Ct. at 2218.

¹³ Sprint, *Sprint Corp. Transparency Report 4* (2018), <http://goodworks.sprint.com/content/1022/files/Transparency%20Report%20January%202018.pdf>; T-Mobile US, Inc., *Transparency Report for 2017* (2018), <https://www.t-mobile.com/content/dam/t-mobile/corporate/media-library/public/documents/TransparencyReport2017.pdf>.

¹⁴ Verizon, *United States Report*, <https://www.verizon.com/about/portal/transparency-report/us-report/>.

II. Acquisition of Real-Time Cell Phone Location Information is a Fourth Amendment Search.

The government's tracking of Mr. O'Donnell's cell phone was a search and, in the absence of a warrant, violated his rights under the Fourth Amendment and the Maine Constitution.¹⁵ The trial court should have reached this conclusion even before the Supreme Court's recent decision in *Carpenter*. In light of *Carpenter*, that result is now clear.

A. The Third-Party Doctrine Does Not Apply to the Location Data at Issue Here.

The government argues in this case that the Defendant lacked a reasonable expectation of privacy in his cell phone location information because the government obtained it from his service provider, and thus "it is a private party, not the government, collecting the data." (State's Br. 9.) Depending on the type of data the government obtained in this case, the government's argument may rest on a factually incorrect premise. And regardless, *Carpenter* makes plain that this position is wrong as a matter of law.

¹⁵ Because the Fourth Amendment provides adequate protection here, there is no need for the Court to address whether article 1, section 5 of the Maine Constitution should be interpreted to provide even more stringent safeguards against unreasonable searches. *See State v. Hutchinson*, 2009 ME 44, ¶ 18 n.9, 969 A.2d 923 ("Although [article 1, section 5] and the corresponding provision in the Fourth Amendment of the United States Constitution generally offer identical protection, we have also recognized that the Maine Constitution may offer additional protections." (citation omitted)); Jamesa J. Drake, *Reviving Maine's State Constitutional Protection Against Unreasonable Searches and Seizures*, 68 Me. L. Rev. 321 (2016).

The record does not make clear the precise nature of the cell phone location data law enforcement obtained from Verizon in this case. At the suppression hearing, Sgt. Austin stated several times that Verizon “pinged” Mr. O’Donnell’s cell phone at law enforcement’s request. (*See* A60, 69; *see also* A97 (testimony of Lisbon Police Officer Jason St. Pierre).) “Pinging” a cell phone generally refers to an affirmative process, carried out at the request of law enforcement, whereby the service provider causes its network to surreptitiously communicate with the target cell phone and thereby derives the device location in real time. *See Maryland Real-Time Order*, 849 F. Supp. 2d at 534–35. Sgt. Austin also stated, however, that Verizon provided “the coordinates of where the cell phones were last on, I guess, if you will.” (A. 62.) Although equivocal, this description could indicate that law enforcement obtained historical location data that was already generated automatically by Verizon and then passed on to law enforcement.¹⁶

If the government in fact obtained real-time “pinging” data, then the location information in this case was not collected by Verizon “in the ordinary course of [its] business.” (State’s Br. 10.) It therefore does not fall within the scope of the

¹⁶ The lack of clarity in Sgt. Austin’s testimony is likely a result of the fact that this was the first time he had obtained real-time cell phone location information, and was not familiar with the procedures involved. (A. 74–76.) Because the third-party doctrine does not apply as a matter of law regardless of which location method was actually used, no further factual development on this point is needed.

“third-party doctrine.”¹⁷ As discussed above, when a service provider receives a request to track a phone in real time, it typically obtains the phone’s location by continuously “pinging” the device. This “pinging” data is “not collected as a necessary part of cellular phone service, nor generated by the customer in placing or receiving a call.” *Maryland Real-Time Order*, 849 F. Supp. 2d at 538 n.6. Under these circumstances, “it is difficult to understand how the user ‘voluntarily’ exposed such information to a third party.” *Id.* at 539 n.6; accord *Tracey v. State*, 152 So. 3d 504, 522–23 (Fla. 2014). Indeed, real-time tracking is quintessentially a case of the government “requiring a third party to collect” information, *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 610 (5th Cir. 2013), which has always constituted a Fourth Amendment search. *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 614 (1989) (“[T]he [Fourth] Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government.”). The United States conceded as much at oral argument in *Carpenter*. Tr. of Oral Arg. at 79, *Carpenter*, 138 S. Ct. 2206 (No. 16-402) (when the government “acquir[es] GPS information . . . from a [cellular] handset[, t]he government reaches into the phone, pulls out information. That, I would concede, is a search.”).

¹⁷ The third-party doctrine is a legal theory asserting that law enforcement can collect some, but not all, types of data that a subscriber voluntarily discloses to a service provider.

In any event, regardless of whether the data was generated at law enforcement request or was recorded by Verizon as a routine matter and turned over to law enforcement shortly thereafter, *Carpenter* holds that the Fourth Amendment applies. In *Carpenter*, the government argued that two cases from the 1970s concerning bank records and a few days of dialed telephone numbers, *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), stood for the blanket proposition that any data obtained by the government from a third-party company falls outside of the Fourth Amendment’s protections. The Supreme Court rejected this position and “decline[d] to extend *Smith* and *Miller* to the collection of CSLI.” *Carpenter*, 138 S. Ct. at 2220. The Court explained that application of the Fourth Amendment must “contend with the seismic shifts in digital technology that made possible the tracking of not only *Carpenter*’s location but also everyone else’s.” *Id.* at 2219. Cell phone location information reflects “a detailed chronicle of a person’s physical presence” and, “[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.” *Id.* at 2220. There is thus a “world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.” *Id.* at 2219. Therefore, “the fact that the Government obtained the information from a third party does not overcome [an individual’s]

claim to Fourth Amendment protection.” *Id.* at 2220. That rule applies squarely to the cell phone location data at issue here.

B. The Warrantless Tracking of Mr. O’Donnell’s Phone Violated His Reasonable Expectation of Privacy.

In *Carpenter*, the Supreme Court addressed a Fourth Amendment challenge to two warrantless requests for a suspect’s historical CSLI, seeking 152 and seven days of records, respectively. *Id.* at 2212. The Court held that there is a reasonable expectation of privacy in this data because it reveals Americans’ “privacies of life” and is “remarkably easy, cheap, and efficient compared to traditional investigative tools,” thus undermining traditional protections against “a too permeating police surveillance.” *Id.* at 2214, 2218 (citations omitted). Although the Court limited its holding to the facts before it, and thus declined to address how the Fourth Amendment would apply to requests for durations of historical CSLI shorter than seven days or to real-time cell phone tracking, *id.* at 2217 n.3, 2220, the Court’s reasoning compels the conclusion that collection of real-time cell phone location data implicates Americans’ reasonable expectations of privacy and requires a warrant. Other courts recognized as much prior to *Carpenter*, and this Court should do so now. *See Tracey v/ State*, 152 So. 3d 504 (Fla. 2014) (warrant required for real-time cell phone location tracking under Fourth Amendment); *United States v. Powell*, 943 F. Supp. 2d 759 (E.D. Mich. 2013) (same); *Maryland Real-Time*

Order, 849 F. Supp. 2d 526 (same); *see also State v. Earls*, 70 A.3d 630 (N.J. 2013) (warrant required for real-time cell phone location tracking under state constitution); *Commonwealth v. Almonor*, No. 1283CR00492 (Plymouth Sup. Ct. Sept. 8, 2016), *appeal pending*, No. SJC-12499 (Mass.) (same).

As explained below, real-time cell phone location tracking violates reasonable expectations of privacy because it reveals private information about presence in constitutionally protected spaces and about locations and movements over time, and because it provides the government with unprecedented new powers that upset people’s well-settled privacy expectations.

1. Real-Time Cell Phone Tracking Reveals Private Information About Presence in Protected Spaces.

As the Supreme Court explained in *Carpenter*, because people carry their cell phones with them virtually everywhere they go, “[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” 138 S. Ct. at 2218; *accord Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (“[N]early three-quarters of smart phone users report being within five feet of their phones most of the time.”). Given the precision of cell phone location data, *see supra* Part I, tracking a cell phone will often reliably place a person within such locations. *Maryland Real-Time Order*, 849 F. Supp. 2d at 540 (noting that “the precision of

GPS and cell site location technology considered in combination with other factors demonstrates that [it] . . . will in many instances place the user within a home, or even a particular room of a home”).

The Supreme Court has repeatedly recognized that the Fourth Amendment draws a “firm” and “bright” “line at the entrance to the house.” *Kyllo*, 533 U.S. at 40 (2001) (citing *Payton v. New York*, 445 U.S. 573, 590 (1980)). This protection extends to other private spaces as well. *E.g.*, *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486–88 (1964) (hotel rooms). In the digital age, the Fourth Amendment’s protections are not limited to physical entry by police; using technology “to explore details of the home that would previously have been unknowable without physical intrusion . . . is a ‘search’ and is presumptively unreasonable without a warrant.” *Kyllo*, 533 U.S. at 40. That rule has been applied to police use of thermal imaging devices that can read heat signatures emanating from the interior of a home, *id.*, as well as to the use of a beeper to track someone into “a private residence.” *United States v. Karo*, 468 U.S. 705, 714 (1984). Even technologies that may be used without a warrant to augment police surveillance in *public* spaces implicate the Fourth Amendment and require a warrant when used to draw inferences about “location[s] not open to visual surveillance,” such as whether an “article is actually located at a particular time in the private residence” or other protected space. *Id.* at 714–15.

Real-time tracking raises these concerns. Mr. O'Donnell's cell phone location data led police to find him inside a room at a motel, a location protected by the Fourth Amendment. (A. 97–99); *see also Earls*, 70 A.3d at 642 (real-time cell phone tracking located defendant “in a motel room”); *Stoner*, 376 U.S. at 486–88; *State v. Oken*, 569 A.2d 1218, 1220 (Me. 1990) (noting parties' agreement that “one may have a reasonable expectation of privacy in one's motel room”). By turning his phone into a tracking device, police learned information about his presence in a constitutionally protected space that they could not otherwise have known. This constitutes a search. *See State v. Andrews*, 134 A.3d 324, 349 (Md. Ct. Spec. App. 2016) (using cell site simulator equipment to locate a cell phone inside a residence is a Fourth Amendment search); *United States v. Lambis*, 197 F. Supp. 3d 606, 610 (S.D.N.Y. 2016) (same).¹⁸

¹⁸ Because “the government cannot know in advance of obtaining this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces,” “[i]t would be impractical to fashion a rule prohibiting a warrantless search only retrospectively based on the fact that the search resulted in locating the cell phone inside a home or some other constitutionally protected area.” *Andrews*, 134 A.3d at 349 (citation omitted). Rather, in order to provide sufficient “guidance” and “deterrence,” a warrant must be *per se* required. *Id.* at 350; *see also Kyllo*, 533 U.S. at 38–39 (requiring warrant for thermal imaging scans of homes because “no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up ‘intimate’ details—and thus would be unable to know in advance whether it is constitutional”).

2. Real-Time Cell Phone Tracking Reveals Private Information About Location and Movement Over Time.

As the Supreme Court explained in *Carpenter*, “[m]apping a cell phone’s location over the course of [time] provides an all-encompassing record of the holder’s whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’” *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). Even when this data does not place a person inside a constitutionally protected space, “[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere.” *Id.* at 2217. Rather, as recognized by five concurring Justices in *United States v. Jones* and reaffirmed by the Court in *Carpenter*, “individuals have a reasonable expectation of privacy in the whole of their physical movements” because of the “privacies of life” those movements can reveal. *Carpenter*, 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); *id.* at 415 (Sotomayor, J., concurring)).

Although *Carpenter* and *Jones* dealt with longer-term location tracking, “[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance . . . will require particular attention. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Like longer-term location data, short-term cell phone location tracking can reveal information “the indisputably private nature of which

takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.” *People v. Weaver*, 909 N.E.2d 1195, 1195 (N.Y. 2009); *see also Carpenter*, 138 S. Ct. at 2218 (“A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.”).

Even if it turns out after the fact that a relatively short period of cell phone tracking data did not reveal anything acutely private, as the Florida Supreme Court has explained, “basing the determination as to whether warrantless real time cell site location tracking violates the Fourth Amendment on the length of the time the cell phone is monitored is not a workable analysis.” *Tracey*, 152 So. 3d at 520. For one, police will often not know at the outset how long they will need to track a suspect’s phone; a suspect may be located after just a few hours, or not for days. And “case-by-case, after-the-fact, ad hoc determinations whether the length of the monitoring crossed the threshold of the Fourth Amendment in each case challenged” will fail to provide adequate guidance to law enforcement at the outset of an investigation. *Id.* Police need “workable rules” to guide their conduct, and the only rule that adequately protects against exploitation of technology to evade the

Fourth Amendment’s protections against pervasive cell phone location monitoring is a clear requirement that police get a warrant. *Id.* at 521.

3. Real-Time Cell Phone Tracking Provides the Government Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy.

In a series of cases addressing the power of “technology [to] enhance[] the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes,” the Supreme Court “has sought to ‘assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34) (last alteration in original); *accord Jones*, 565 U.S. at 406. As Justice Alito explained in *Jones*, “[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.” 565 U.S. at 429 (Alito, J., concurring in judgment). Accordingly, the Court has remained vigilant “to ensure that the ‘progress of science’ does not erode Fourth Amendment protections.” *Carpenter*, 138 S. Ct. at 2223.

Thus, the Supreme Court has held that police must obtain a warrant before using a thermal imager to observe details about the interior of a home that, prior to the availability of the technology, would have been shielded from view as a practical matter. *Kyllo*, 533 U.S. at 35. Likewise, a warrant is required to search the contents of a phone seized incident to arrest because the traditional rule permitting

warrantless searches incident to arrest fails to “strike[] the appropriate balance” given the “immense storage capacity” of modern cell phones. *Riley*, 134 S. Ct. at 2484, 2489.

In the context of location tracking, while historically police could have engaged in “relatively short-term monitoring of a person’s movements on public streets,” “[t]raditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.” *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in judgment). GPS tracking, however, “make[s] long-term monitoring relatively easy and cheap.” *Id.* at 429. Therefore, “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” *Id.* at 430. Similarly, access to historical CSLI “is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.” *Carpenter*, 138 S. Ct. at 2217–18. Whereas, “[i]n the past, attempts to reconstruct a person’s movements were limited by a dearth of records and the frailties of recollection[, w]ith access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts.” *Id.* at 2218. Warrantless access to historical CSLI therefore violates people’s reasonable expectations of privacy.

Real-time cell phone location tracking, even over a short period, likewise provides the government with an unprecedented power that upends traditional expectations of privacy. Prior to the cell phone age, police “had the capacity to visually track a suspect from some starting location, and electronic tracking devices . . . [like beepers and GPS devices] have augmented this preexisting capacity.” *Prince Jones v. United States*, 168 A.3d 703, 712 (D.C. 2017). That power has always been limited, however, by the need for police to know where they could find the suspect, so they could either surveil that person visually or install a tracking device “on some object that the target will later acquire or use.” *Id.* Today, by contrast, police can locate a person without knowing in advance where or even who they are, by “remotely activat[ing] the latent tracking function of a device that the person is almost certainly carrying in his or her pocket or purse: a cellphone.” *Id.*; see also *United States v. Skinner*, 690 F.3d 772, 786 (6th Cir. 2012) (Donald, J., concurring in part and concurring in the judgment) (when they began tracking the suspect’s cell phone, “[a]uthorities did not know the identity of their suspect, the specific make and model of the vehicle he would be driving, or the particular route by which he would be traveling.”). Police can pluck a suspect’s precise location out of thin air, with no more information than that person’s cell phone number. See *Tracey*, 152 So.3d at 525 (“[L]aw enforcement did not know of Tracey’s whereabouts on the public roads and, thus, could not

track him by visual observation. Officers learned of his location on the public roads, and ultimately inside a residence, only by virtue of tracking his real time cell site location information emanating from his cell phone.”). The power of the government “not merely to *track* a person but to *locate* him or her” cheaply, easily, and precisely violates expectations of privacy by providing police with an unprecedented capability which, without regulation, is prone to abuse. *Prince Jones*, 168 A.3d at 712. Thus, even shorter-term use of cell phone tracking data to locate a person whose whereabouts were otherwise unknown to police is a search that requires a warrant.

C. The Warrantless Tracking of Mr. O’Donnell’s Phone Interfered with the Security of His Person, Papers, and Effects.

As in *Carpenter*, this case can be resolved by reference to the familiar reasonable-expectation-of-privacy test. *See Carpenter*, 138 S. Ct. at 2213–14; *supra* Part II.B. Should the Court wish, however, this case can also be analyzed under a “property-based approach.” *Jones*, 565 U.S. at 405, 409 (“[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.”). That approach, like the privacy-based approach discussed above, leads to the conclusion that law enforcement’s tracking of Mr. O’Donnell’s cell phone was a Fourth Amendment search.

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” As the Supreme Court has explained, at a minimum, “[w]hen the Government obtains information by physically intruding on persons, houses, papers, or effects, a search within the original meaning of the Fourth Amendment has undoubtedly occurred.” *Florida v. Jardines*, 569 U.S. 1, 5 (2013) (quotation marks omitted) (citing *Jones*, 565 U.S. at 406 n.3).

Thus, in *Jones*, the Supreme Court held that “the Government’s installation of a GPS device on a target’s vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a ‘search.’” 565 U.S. at 404. That is so because the attachment of the GPS device to the defendant’s car without consent was a common-law trespass to chattels. *Id.* at 405, 426. Because a vehicle is an “effect” within the meaning of the Fourth Amendment, the government’s installation of this device “encroached on a protected area.” *Id.* at 404, 410. The Court has likewise held that the government conducts a search “when it attaches a [GPS monitoring] device to a person’s body, without consent, for the purpose of tracking that individual’s movements,” *Grady v. North Carolina*, 135 S. Ct. 1368, 1370 (2015) (per curiam), and when it “physically intrudes on the curtilage [of a home] to gather evidence.” *Collins v. Virginia*, 138 S. Ct. 1663, 1670 (2018) (citing *Jardines*, 569 U.S. at 11).

Here, the government’s warrantless tracking of Mr. O’Donnell’s cell phone interfered with the security of, and his property interests in, his person, his papers (his location data), and his effects (his cell phone).

First, cell phones “are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.” *Riley*, 134 S. Ct. at 2484. Indeed, survey data indicates that “nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.” *Id.* at 2490. That is why the Court in *Carpenter* explained that “when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s use.” 138 S. Ct. at 2218. This is no mere simile. By transforming Mr. O’Donnell’s cell phone into a real-time tracking device, the government effectively installed a tracking beacon on his person. This interfered with his bodily autonomy and constitutes a search. *See Grady*, 135 S. Ct. at 1370 (attaching GPS ankle monitor to a person is a Fourth Amendment search); *Carpenter*, 138 S. Ct. at 2218 (in the absence of “the constraints of the Fourth Amendment,” “[o]nly the few without cell phones could escape this tireless and absolute surveillance”).

Second, “cell phones are ‘effects’ as that term is used in the Fourth Amendment.” *Tracey*, 152 So. 3d at 524. When the government requested that

Mr. O’Donnell’s service provider begin tracking the phone in real time, it effectively sought to “hijack[] the phone’s GPS.” *In re Application*, 724 F.3d at 615. In doing so, it interfered with his control over his phone by transforming it from a communications tool into a government tracking device. In effect, the government “usurp[ed]” Mr. O’Donnell’s property, *Silverman v. United States*, 365 U.S. 505, 511 (1961), by divesting him of his “right to exclude others” from obtaining data from the phone. *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (“One of the main rights attaching to property is the right to exclude others.”). In property-law terms, this was a conversion of Mr. O’Donnell’s chattel: an “act of dominion wrongly exerted over property in denial of the owner’s right, or inconsistent with it.” *McPheters v. Page*, 83 Me. 234, 22 A. 101, 102 (1891). Like the trespass to chattels in *Jones*, the conversion of Mr. O’Donnell’s property for the purpose of gathering information was a search.

Finally, the warrantless acquisition of Mr. O’Donnell’s cell phone location data interfered with the security of his papers. In his dissenting opinion in *Carpenter*, Justice Gorsuch explained his view that private and sensitive records in the hands of a third party can fall under the Fourth Amendment’s protection of a person’s “papers.” 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting). This is so even when control of and proprietary interest in those records is divided between the individual to whom they pertain (i.e., Mr. O’Donnell) and the business with

custody of them (i.e., Verizon). *Id.* at 2269. In order to determine whether a person has an interest in data held by a third party sufficient to trigger the Fourth Amendment’s protections, Justice Gorsuch would look to positive law—state and federal legislation and common law protections that shield certain types of data from nonconsensual disclosure or use. *Id.* at 2270.

Here, cell phone location information is heavily protected by law, thus vesting cell phone users with a Fourth Amendment interest in that data. Maine, like at least ten other states, requires a warrant for law enforcement access to real-time cell phone location data. 16 M.R.S. § 648; *accord* Cal. Penal Code § 1546.1(b); 725 Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Md. Code Ann. Crim. Proc. § 1-203.1(b); Minn. Stat. § 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); N.H. Rev. Stat. Ann. § 644-A:2; 12 R.I. Gen. Laws § 12-32-2; Utah Code Ann. § 77-23c-102(1)(a); Vt. Stat. Ann. tit. 13, § 8102(b); *see also* Kan. Stat. Ann. § 22-2502(a)(1)(G)(i).

Federal law also protects the data. Congress has prohibited law enforcement from tracking the location of a cell phone using the federal pen register statute, 18 U.S.C. § 3127, which is the means for authorizing real-time monitoring of other telephony metadata. 47 U.S.C. § 1002(a)(2) (“call-identifying information” acquired under the pen register statute “shall not include any information that may disclose the physical location of the subscriber”). As a result, federal law

enforcement agents must use a search warrant to track a cell phone in real time. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005). In addition, the federal Telecommunications Act requires “express prior authorization of the customer” before a service provider can “use or disclose . . . call location information,” 47 U.S.C. § 222(f), and provides “customers a private cause of action for damages against carriers who violate the Act’s terms.” *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) (citing 47 U.S.C. § 207). Federal law also criminalizes obtaining or attempting to obtain phone location information by making false or fraudulent statements. 18 U.S.C. § 1039 (a).

As a result of these protections, “customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use.” *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). Those interests create a property right in the data, and make nonconsensual and warrantless access by law enforcement a Fourth Amendment search.

D. In the Absence of Exigent Circumstances, Real-Time Cell Phone Location Tracking Requires a Warrant.

As this Court has repeatedly explained, “[w]arrantless searches are *per se* unreasonable, subject to a few specifically established, carefully drawn and much guarded exceptions.” *Oken*, 569 A.2d at 1220 (quoting *State v. Philbrick*, 436 A.2d

844 (Me.1981)). Thus, “[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.” *Carpenter*, 138 S. Ct. at 2221 (quoting *Riley*, 134 S. Ct. at 2482). As applied to cell phone tracking, the warrant requirement both is required by the Fourth Amendment, and is eminently reasonable. Indeed, the FBI has advised its agents since at least 2011 that a “search warrant should be obtained to compel the disclosure of . . . [real-time] geo-location data” from a service provider.¹⁹

Although “case-specific” exigent circumstances, such as “the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence,” can supply an exception to the warrant requirement, *id.* at 2222–23, here the trial court properly determined that “law enforcement in this case were not reasonable in their belief that an emergency . . . required disclosure of the location information without delay.” (A. 26.) The government does not contest this holding. (State’s Br. 10.) Accordingly, if this Court holds that the tracking of Mr. O’Donnell’s cell phone was a search, it should also find that doing so without a warrant was unreasonable, and therefore violated his Fourth Amendment rights.

¹⁹ Fed. Bureau of Investigation, *Domestic Investigations and Operations Guide* § 18.6.8.4.2.5.3, at 18-113–14 (2011).

III. The Legislature Intended to Provide a Suppression Remedy for Violations of 16 M.R.S. § 648.

As described above, the Superior Court’s decision conflicts with *Carpenter*, 138 S. Ct. at 2206, and must be reversed. A decision solely based on *Carpenter*, however, could inadvertently imply that the Superior Court’s interpretation of existing Maine statutory law concerning location privacy was correct. It was not. By holding there was no exclusionary remedy for Maine statute’s prohibition against warrantless collection of cell phone location data, 16 M.R.S. § 647 *et seq.*, the Superior Court misinterpreted Maine law. This Court would do a service to the Maine legislature in acknowledging as much, in order to protect and promote comity among the branches of government. And, it would do a service to the Maine people, so that they would be reassured that their own laws are interpreted and applied fairly and consistently by the courts.

The Superior Court’s errors were related to both the method of interpretation and the interpretation itself. With regard to methodology, the Superior Court disregarded the clear instruction of this Court (in addition to longstanding interpretative principles) regarding the proper way to interpret a statute. The role of Maine courts in construing statutes is to discern and give effect to the Legislature’s intent. *Ford Motor Co. v. Darling’s*, 2016 ME 171, ¶ 24, 151 A.3d 507. The first source for that intent is the “statute’s plain meaning and the entire statutory scheme of which the provision at issue forms a part.” *Id.* (citing *Samsara Mem’l Trust v.*

Kelly, Remmel & Zimmerman, 2014 ME 107, ¶ 42, 102 A.3d 757). The first (and in most cases, only) step in this analysis is consideration of the statute’s plain language, giving meaning to all words and not treating any words as surplusage if they can be reasonably construed. *See Hickson v. Vescom Corp.*, 2014 ME 27, ¶ 15, 87 A.3d 704.

The Superior Court followed this direction in determining whether a warrant was required. (A. 24.) Under Maine law, the police were not permitted to obtain information about the location of an electronic device without a valid warrant unless there is an emergency. 16 M.R.S. §§ 648, 650(4). The court reasoned (correctly) that location information had been obtained, no warrant had been issued, and there had been no emergency. (A. 24–28.) Therefore, the location information had been illegally obtained, in contradiction with Maine law. But, when it came to analyzing what to do about the illegally obtained location information, the Superior Court diverged from the plain meaning of the statute and went searching for legislative intent in the tangled legislative history.

Consideration of extrinsic evidence in statutory interpretation, such as legislative history, is only appropriate when the meaning of the statute is ambiguous—that is, the plain language of the statute, read in light of the entire statutory scheme of which it is a part, is subject to at least two reasonable alternative interpretations. *See Maine Today Media, Inc. v. State*, 2013 ME 100,

¶ 6, 82 A.3d 104. Here, the statutory language governing the use of location information was not in the least bit ambiguous. It states quite clearly that location information, or evidence derived from that information, may only be received in evidence if a copy of the warrant and accompanying application is provided to each party to the proceeding. 16 M.R.S. § 650-A(1); *accord* M.R.U. Crim. P. 41B(c)(6) (“[U]se at a trial, hearing, or proceeding of location information or evidence derived from it is conditioned upon notice and the furnishing of certain warrant materials as provided by 16 M.R.S. § 650-A(1).”). Mr. O’Donnell was never provided a copy of the warrant authorizing the disclosure of his cell-phone location information because no such warrant existed. Therefore, both location data and related evidence were inadmissible.²⁰

The Superior Court observes that § 650-A(1) does not employ the phrase “exclusionary rule,” and this is indeed correct. But there is no requirement for magic words to accomplish the goal of exclusion. The legislature clearly indicated that location information may be received in evidence “only if” there is compliance with the statutory requirement to obtain a warrant and furnish a copy of it to the

²⁰ The judicial waiver provision at 16 M.R.S. § 650-A(2) permits a judge to waive the requirement that a location tracking warrant be provided to the defendant not less than 10 days before trial. By its plain terms, that provision applies only to the timing of the government’s obligation to provide of a copy of the warrant. It does not apply in cases like this one where no warrant was obtained and therefore no warrant can be furnished to the defense at all.

defense.²¹ 16 M.R.S. § 650-A(1). The warrant requirement was not satisfied here, so the evidence must be excluded. *Id.*

The Superior Court also observes that the legislature considered a number of possible phrasings for § 650-A(1), and this is also correct. But the job of the Superior Court was not to provide a selective history of the crafting of Maine’s location privacy statute—a history in which Justice Stokes was no mere passive observer²²—but rather to construe the language of the statute as enacted. The history of discarded phrases and committee vote totals that the Superior Court relies upon is, in fact, indicative of nothing. *See Mahaney v. Miller’s, Inc.*, 669 A.2d 165, 169 (Me. 1995); *see also Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 187 (1994) (“[Legislative] inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction.”). The Superior Court inappropriately substituted selective excerpts from the legislative history and portions of bill and amendment summaries for the unambiguous language of the statute itself. But, it is the

²¹ Indeed, had it so intended, the legislature could easily have opted not to provide for exclusion of evidence as a remedy for violation of the warrant and notice requirements. *Compare* 12 R.I. Gen. Laws § 12-32-3 (f) (in statute requiring that cell phone location warrants be served on the cell phone user within a specified period of time, providing that “[f]ailure to comply with the notice provisions shall not be grounds for the suppression of any evidence”).

²² *See An Act To Require a Warrant To Obtain the Location Information of a Cell Phone or Other Electronic Device: Hearing on L.D. 415 Before the J. Standing Committee on Judiciary*, 126th Legis. (2013) (testimony of Deputy Attorney General William R. Stokes, Chief of Attorney General’s Criminal Division), *available at* <https://mainelegislature.org/legis/bills/getTestimonyDoc.asp?id=4616>.

“statutory language, plain on its face” that courts are charged with interpreting, not public testimony, legislative debate, or bill summaries. *See Stone v. Bd. of Registration in Med.*, 503 A.2d 222, 227 (Me. 1986). “To depart from the controlling text of [the Act] in search of an alternative interpretation would amount to rewriting the law enacted by the legislature.” *Id.* at 228.

Nor is it relevant that the Governor vetoed L.D. 415 when it was presented to him by the legislature. (A. 29.) Bills that are vetoed by the Governor but subsequently passed by two-thirds of both houses “shall have the same effect as if it had been signed by the Governor.” Me. Const. art. IV, pt. 3, § 2. Maine’s cell-phone location privacy law was lawfully enacted and codified, and the legislature intended for it to be enforced.

The Superior Court’s use of legislative history here is the “equivalent of entering a crowded cocktail party and looking over the heads of the guests for one’s friends.” *Conroy v. Aniskoff*, 507 U.S. 511, 519 (1993). The Superior Court simply cannot selectively invoke portions of an “ambiguous legislative history to muddy clear statutory language.” *Milner v. Dep’t of Navy*, 562 U.S. 562, 572 (2011). In issuing its decision on *Carpenter*, amici ask that the Court also acknowledge Maine’s important statutory protections for location data, including the exclusionary remedy for those protections.

CONCLUSION

For the foregoing reasons, Amici respectfully urge the Court to hold that warrantless real-time tracking of Mr. O'Donnell's cell phone constituted a search under the Fourth Amendment and under article 1, section 5 of the Maine Constitution, and that violation of the warrant and notice requirements in 16 M.R.S. §§ 648 and 650-A should result in the suppression of evidence.

August 30, 2018

Respectfully submitted,

/s/ Zachary L. Heiden
Zachary L. Heiden (#9476)
American Civil Liberties Union
of Maine Foundation
121 Middle Street, Suite 200
Portland, ME 04101
(207) 619-8687
Counsel for Amici Curiae

Nathan Freed Wessler
Jennifer Stisa Granick
Brett Max Kaufman
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
Of Counsel

Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
Of Counsel

Tina Heather Nadeau, Esq.,
Bar No. 4684
Executive Director
Maine Association of Criminal Defense
Lawyers
P.O. Box 17642
Portland, ME 04112-8642
*Counsel for Amicus Curiae Maine
Association of Criminal Defense
Lawyers*

CERTIFICATE OF SERVICE

I, Zachary L. Heiden, hereby certify that on August 30, 2018, two copies of this brief were served via first-class mail to each of the following counsel:

Counsel for the Appellant:

Adam P. Sherman, Esq.
Paradie, Sherman, Walker & Worden, P.A.
217 Main Street, Suite 400
Lewiston, ME 04240

Counsel for the Appellee:

Claire Gallagan Andrews, Assistant District Attorney
Office of the District Attorney
District III—Franklin County
124 Maine Street, Suite 105
Farmington, ME 04938

Dated at Portland, Maine this 30th day of August, 2018.

/s/ Zachary L. Heiden
Zachary L. Heiden (#9476)
American Civil Liberties Union
of Maine Foundation
121 Middle Street, Suite 200
Portland, ME 04101
(207) 619-8687
Counsel for Amici Curiae

STATE OF MAINE

SUPREME JUDICIAL COURT

Sitting as the Law Court

Docket No. Fra-17-12

State of Maine

v.

CERTIFICATE OF SIGNATURE

Kevin O'Donnell

You must file this certificate if you do not sign at least one paper copy of your brief. This form may be used only by an attorney representing a party.

I am filing the electronic copy of a brief with this certificate. I will file the paper copies as required by M.R. App. P. 7A(i). I certify that I have prepared (or participated in preparing) the brief and that the brief and associated documents are filed in good faith, conform to the page or word limits in M.R. App. P. 7A(f), and conform to the form and formatting requirements of M.R. App. P. 7A(g).

Name(s) of party(ies) on whose behalf the brief is filed: American Civil Liberties Union of Maine, American Civil Liberties Union, Electronic Frontier Foundation, Maine Association of Criminal Defense Lawyers

Attorney's name: Zachary L. Heiden

Attorney's Maine Bar No.: 9476

Attorney's email address: heiden@aclumaine.org

Attorney's street address: 121 Middle Street, Ste. 200, Portland, ME 04101

Attorney's business telephone number: (207) 619-8687

Date: August 30, 2018

No signature is required on this document. The electronic transmission of this document to the Clerk serves as the attorney's signature.