Received 9/21/2020 3:29:04 PM Supreme Court Middle District

Filed 9/21/2020 3:29:00 PM Supreme Court Middle District
42 MAP 2020

IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

No. 42 MAP 2020

COMMONWEALTH OF PENNSYLVANIA,
Appellee,

v.

DAVID PACHECO,
Appellant.

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT DAVID PACHECO

Appeal from the Order and Opinion of the Superior Court, 151 EDA 2018, dated January 24, 2020, affirming the Final Judgment of Sentence entered on November 29, 2017, by the Montgomery County Court of Common Pleas, Criminal Division, No. CP-46-CR-0002243-2016

Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union
of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19102
(215) 592-1513 x138
achristy@aclupa.org

Counsel for Amici Curiae
(Additional Counsel Listed on Following Page)

On the Brief:

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

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONS & STATUTES

REGULATIONS

OTHER AUTHORITIES

STATEMENT OF INTEREST OF AMICI CURIAE

The **American Civil Liberties Union** ("ACLU") is a nationwide, non-profit, non-partisan organization dedicated to defending the civil liberties and civil rights guaranteed by the Constitution. The **American Civil Liberties Union of Pennsylvania** ("ACLU of Pennsylvania"), is a state affiliate of the ACLU. The ACLU and ACLU of Pennsylvania 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 8 of the Pennsylvania 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 **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 Pennsylvania, 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*, 138 S. Ct. 2206; *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).[1]

SCOPE OF AMICUS BRIEF

Addressing only issue b. set forth in this Court's grant of allocatur, this brief argues "that the decision of the United States Supreme Court in *Carpenter v. United States*, 138 S.Ct. 2206 (2018), extends to the collection of real time cell site location information."[2] Order granting allocatur (July 28, 2020). As to issue a., *amici* agree with Defendant-Appellant that the standard for issuance of an order under 18 Pa.C.S. § 5773 does not meet the probable cause requirement under the Fourth Amendment and Article I, Section 8, and therefore the real-time tracking order in this case was not the functional equivalent of a warrant. *Amici* respectfully refer the Court to the brief of *amicus curiae* the Public Defender Association of Pennsylvania for argument on that issue. *Amici* further urge that even if the Court rules for the government on issue a., it announce a decision on issue b., which

[1] No other person or entity paid for or authored this Brief.

[2] As described below, this case involves tracking a phone by causing it to calculate and transmit its GPS coordinates, which is technologically distinct from—and more precise than—the cell site location information at issue in *Carpenter*.

involves an issue of great importance to residents of this state.

SUMMARY OF ARGUMENT

For nearly every American and Pennsylvanian, cell phones have 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 his 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. 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. Because of the high sensitivity of cell phone location data, the unavoidability of its creation, and

its ability to reveal the whole of a person's movements over time, the Fourth Amendment's protections apply.

Just 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. Like acquiring historical cell phone data, 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). Moreover, the GPS coordinates obtained here—markedly more precise than the cell site records at issue in *Carpenter*— can 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 (citation omitted), 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 and follow them ceaselessly and without detection. In order to prevent this capability from feeding a

"too permeating police surveillance," *id.* (citation omitted), the Fourth Amendment's warrant requirement applies.[3]

Alternatively, real-time cell phone location tracking implicates the Fourth Amendment because, by forcing a person's cell phone to transmit its coordinates, the government reduces that person to a trackable object, converts the 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).

Finally, even if real-time cell phone tracking were not a search under the Fourth Amendment, it would be a search under Article I, Section 8. This Court has long made clear that the State Constitution protects privacy to an even greater degree than does the Fourth Amendment. Like pen register information and bank records, which require a warrant under Article I, Section 8, real-time cell phone location information reveals numerous private details of people's lives, and is protected by a reasonable expectation of privacy. Therefore, police must secure a warrant before compelling a phone company to track a person's phone.

[3] Of course, when law enforcement agents have probable cause but exigent circumstances prevent them from applying for a warrant, they may proceed without one. *Carpenter*, 138 S. Ct. at 2222–23. But in a case like this, where no such exigency existed, a warrant is required.

ARGUMENT

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

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, and can continue the tracking day and night for weeks or months.

This capability stems from rules first adopted in 1996 and fully implemented in the early 2000s, under which the Federal Communications Commission ("FCC") required cellular service providers to be able to identify "the location of all 911 calls by longitude and latitude." 47 C.F.R. § 9.10(e). 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, 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. *Id.* § 9.10(i).

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. In doing so, law enforcement agents "can specify the interval at which location results are generated," (Sprint Certification, R.R. 575a), and can receive the location information contemporaneously via email or text, (*id.*), or 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 powered on and 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).[4] 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.

[4] *E.g. E911 Compliance FAQs*, Verizon Wireless, http://www.verizonwireless.com/support/e911-compliance-faqs.

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 carrier's network: (1) by using Global Positioning System ("GPS") hardware built into the phone ("handset-based" technology); and/or (2) by triangulating the phone's location based on the phone's interactions with the network's cellular towers, or "cell sites" ("network-based" technology).[5] Both methods are mandated by federal regulations to produce precise location coordinates. *See* 47 C.F.R. § 9.10(h)–(i).

Handset-based technology uses a mobile device's "special hardware that receives signals from a constellation of global positioning satellites."[6] The GPS chip installed in a cellular telephone uses radio signals from GPS satellites orbiting Earth to calculate its own location within ten meters.[7] Newer receivers, with enhanced communication to ground-based technologies that correct signal errors, can specify location within three meters or closer, and have a vertical accuracy of

[5] Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy & Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary, 113th Cong. 45 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ("Blaze Hearing Statement"), *available at* https://fas.org/irp/congress/2013_hr/ecpa2.pdf.

[6] *Id.* at 51; *see also* 47 C.F.R. § 9.3.

[7] Blaze Hearing Statement at 51; *see also In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 540–41 (D. Md. 2011) [hereinafter "*Maryland Real-Time Order*"] (noting that GPS-derived cell phone location data can be precise enough to locate a cell phone within a residence).

five meters or better ninety-five percent of the time.[8] In this case, the tracking of Mr. Pacheco's phone at times returned results accurate to within nine meters. (Suppression Hr'g Tr., 4/10/17, R.R. 208a.)

As occurred in this case, upon law enforcement request, service providers can remotely activate a phone's GPS functionality and then cause the phone to transmit its coordinates back to the provider. (*Id.*, R.R. 202a, 217a–218a; Sprint Certification, R.R. 575a); *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." *Maryland Real-Time Order*, 849 F. Supp. 2d at 531, 534–35 (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.[9]

---

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

[9] Blaze Hearing Statement at 60–61; 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).

Service providers can obtain this triangulated 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.

The power to track and locate any person's cell phone affects virtually all Pennsylvanians. Ninety-six percent of Americans now own cell phones,[10] 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.", 138 S. Ct. at 2218. Across the nation, the government invokes this *Carpenter* power with frequency. Sprint and T-Mobile, for example, respectively received 60,563 and 27,803 real-time cell phone location requests from law enforcement in 2019.[11]

[10] *Mobile Fact Sheet*, Pew Research Center (June 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/; *see also Carpenter*, 138 S. Ct. at 2218.

[11] Sprint, *Sprint Corp. Transparency Report* 4 (2020), https://newsroom.sprint.com/csr/content/1214/files/Transparency%20Report%20January%202020.pdf; T-Mobile US, Inc., *Transparency Report for 2019* (2020), https://www.t-mobile.com/news/_admin/uploads/2020/07/2019-Transparency-Report-3.pdf.

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

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

In *Carpenter*, the Supreme Court made clear that because cell phone location information reflects "a detailed chronicle of a person's physical presence" and because, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data," "the fact that the Government obtained the information from a third party does not overcome [an individual's] claim to Fourth Amendment protection." 138 S. Ct. at 2220. That analysis was necessary to address the government's contention that historical cell site location information, which is logged and retained in the normal course of business when cell phone users communicate with the network, *id.*, is a business record of the service provider and not the private information of the user.

If the GPS data at issue were routinely captured and logged by the service provider for its own business purposes and then turned over to the government upon request, *Carpenter* would control and would foreclose any application of the third-party doctrine.[12] But here, real-time tracking simply does not even implicate the third-party doctrine at all. As discussed above, when a service provider

[12] 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.

receives a law enforcement request to track a phone in real time, it typically obtains the phone's location by forcing the device to send its GPS coordinates to the provider, or by continuously "pinging" it. The GPS and "pinging" data are "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. "[W]hen the police ping a cell phone, as they did in this case, they compel it to emit a signal, and create a transmission identifying its real-time location information. This action and transmission is initiated and effectively controlled by the police." *Commonwealth v. Almonor*, 120 N.E.3d 1183, 1193 (Mass. 2019) (citation omitted)). Under these circumstances, it is simply inaccurate to suggest that "the user 'voluntarily' exposed such information to a third party." *Maryland Real-Time Order*, 849 F. Supp. 2d at 538 n.6; *accord Tracey v. State*, 152 So. 3d 504, 522–23 (Fla. 2014). 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 Execs.' 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."). Thus, although *Carpenter* makes clear that the reasonable expectation of privacy in longer-term cell phone location information is not undermined by the phone company's possession of that data, this Court need not even engage in that analysis to find that the real-time tracking qualifies as a search here.

B. The Warrantless Tracking of Mr. Pacheco's Phone Violated His Reasonable Expectation of Privacy.

There is no reason to treat historical and real-time cell phone location information differently under the Fourth Amendment. Like the historical cell site location information at issue in *Carpenter*, real-time 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.

Indeed, many courts recognized the extraordinary privacy intrusion inflicted by real-time cell phone tracking prior to *Carpenter*. *See Tracey*, 152 So. 3d 504 (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. Rushing*, 71 A.3d 939, 963 (Pa. Super. Ct. 2013) (same), *rev'd on other grounds*, 99 A.3d 416 (Pa. 2014). And in the two years since *Carpenter* was decided, courts have expressed "no difficulty in extending the rationale of *Carpenter* as applied to historical CSLI to prospective orders." *State v. Brown*, 202 A.3d 1003, 1014 n.9 (Conn. 2019); *accord State v. Muhammad*, 451 P.3d 1060, 1071 (Wash. 2019) ("*Carpenter*'s reasoning applies to real-time CSLI"); *Sims v. State*, 569 S.W.3d 634, 645 (Tex. Crim. App. 2019); *Almonor*, 120 N.E.3d at 1194–95.

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*, 573 U.S. 373, 395 (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 the cell phone location data at issue in this case, *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 (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 by "exposing a cell phone user's attendance at a location a person would reasonably expect to be private." *Muhammad*, 451 P.3d at 1070. 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).[13]

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

[13] 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"). In any case, persistent location tracking even in public places constitutes "too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214. *See Infra* Part II.B.2.

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 *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); *Riley*, 573 U.S. at 403). The duration of tracking in this case—108 days[14]—is more than enough to create the "all-encompassing record of the holder's whereabouts" that so concerned the *Carpenter* Court. 138 S. Ct. at 2217.

Although *Carpenter* and *Jones* dealt with longer-term location tracking,[15] "[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). Over any timeframe, the precision of real-time cell phone location information will risk revealing information "the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist,

[14] Although the government ended up tracking Mr. Pacheco's phone for 108 days, it obtained authorization for 120 days of tracking. (*Compare* Trial Tr., 8/8/17, R.R. 816a (summarizing 108 days of tracking data), *with* Order 8/28/2015, R.R. 354a (60-day authorization) *and* Order 10/15/2015, R.R. 392a–444a (60-day extension)).

[15] In *Carpenter*, the Court addressed a request for seven days' worth of cell site location information. 138 S. Ct. at 2212, 2217 n.3. In *Jones*, the Court addressed the 28-day use of a GPS tracker attached to a vehicle. 565 U.S. at 403.

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, 1199 (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."). While the months of tracking in this case obviously implicated Mr. Pacheco's "privacies of life," *Carpenter*, 138 S. Ct. at 2217, this Court should take care not to suggest that shorter durations of real-time tracking would evade constitutional regulation.[16]

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

[16] Moreover, "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; police may glean useful information after just a few hours, or may continue monitoring for weeks or months. 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 "workable rules" to law enforcement at the outset of an investigation. *Id.* at 520–21; *Muhammad*, 451 P.3d at 1072–73 ("There is no rational point to draw the line; it is arbitrary and unrelated to a reasonable expectation of privacy.").

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.

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. Like attaching a GPS device to a car, enabling real-time cell phone location tracking, "is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can [follow a person] at practically no expense." *Carpenter*, 138 S. Ct. at 2217–18.

Even over a short period, cell phone tracking 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 and follow them for as long as they wish. *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. Pacheco's Phone Interfered with the Security of His Person, Papers, and Effects.

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. Pacheco'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." U.S. Const. amend. IV. 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).

Here, the government's warrantless tracking of Mr. Pacheco's cell phone interfered with the security of, and his property interests in, his person, his papers (the location data generated on his phone), 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*, 573 U.S. at 385. By transforming Mr. Pacheco's cell phone into a real-time tracking device, the government effectively installed a tracking beacon on his person. *Cf. Grady v. North Carolina*, 575 U.S. 306, 307–08 (2015) (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. 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. When the government requested that Mr. Pacheco'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. In effect, the government "usurp[ed]" Mr. Pacheco'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. Pacheco's chattel: "an act of interference with the dominion or control over a chattel" "without the owner's consent and without lawful justification." *Stevenson v. Econ. Bank of Ambridge*, 197 A.2d 721, 726 (Pa. 1964) (citations omitted). Like the trespass to chattels in *Jones*, the conversion of Mr. Pacheco's property for the purpose of gathering information was a search.

Finally, the warrantless acquisition of Mr. Pacheco'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 and the business with access to them. *Id.* at 2269. In order to determine whether a person has an interest in data held by or generated via 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, 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). Consumer protection statutes prohibit smartphone app providers from using and reselling customer location data in ways that violate customers' rights to appropriately understand and consent to such uses. *See, e.g.*, Press Release, L.A. City Attorney, *City Attorney Feuer Settles Digital Privacy Lawsuit Against the Weather Channel App* (Aug. 19, 2020), https://www.lacityattorney.org/post/city-

attorney-feuer-settles-digital-privacy-lawsuit-against-the-weather-channel-app; Press Release, Fed. Trade Comm'n, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers* (Dec. 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived. And the federal Communications Assistance for Law Enforcement Act, which otherwise requires phone companies to build lawful intercept and surveillance capabilities into their networks, prohibits use of the federal pen register statute to obtain "any information that may disclose the physical location of the subscriber['s cell phone]." 47 U.S.C. § 1002(a)(2).

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.

III. Acquisition of Real-Time Cell Phone Location Information Is a Search Under Article I, Section 8.

Even if warrantless cell phone tracking did not violate the Fourth Amendment, it would still run afoul of Article I, Section 8 of the State Constitution. As this Court has repeatedly explained, "'[t]he notion of privacy in Article I, § 8 is greater than that of the Fourth Amendment,' and, when compared

to federal courts, Pennsylvania courts 'have given greater weight to an individual's privacy interests when balancing the importance of privacy against the needs of law enforcement.'" *Commonwealth v. Arter*, 151 A.3d 149, 157–58 (Pa. 2016) (alteration in original) (quoting *Commonwealth v. McCree*, 924 A.2d 621, 626–27 (Pa. 2007)). Notably, this Court has rejected the third-party doctrine first announced by the U.S. Supreme Court in *United States v. Miller*, 425 U.S. 435 (1976), as "a dangerous precedent, with great potential for abuse" and has "decline[d] to follow that case when construing the state constitutional protection against unreasonable searches and seizures." *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979).

In 1979, the U.S. Supreme Court held that under the Fourth Amendment, the use of a pen register to record the phone numbers dialed on a person's phone line was not a search because the information was voluntarily conveyed to the phone company, and therefore not private. *Smith v. Maryland*, 442 U.S. 735 (1979). A decade later, this Court declined to adopt that reasoning under Article I, Section 8. *Commonwealth v. Melilli*, 555 A.2d 1254 (Pa. 1989). Recognizing the privacy harm of "intrusions into telephone communications," this Court held that "[t]elephone activities are largely of one piece, and efforts to create distinctions between numbers and conversational content are constitutionally untenable in our view." *Id.* at 1258–59. Pen register information falls "within the confines of an

expectation of privacy under the State Constitution and thereby [is] subject to the requirements demonstrating probable cause." *Id.* at 1258. In reaching this conclusion, this Court adopted the reasoning of the Superior Court in *Commonwealth v. Beauford*, 475 A.2d 783, 791 (Pa. Super. Ct. 1984), which explained that unfettered police access to the many private details revealed by learning who a person calls would constitute "a powerful weapon threatening invasion not only of the individual's intimate privacy, but also his political liberty, including his rights to associate, to express his views, and even to think in freedom."

Like the land-line phones in *Melilli*, "[t[he cell phone has become a ubiquitous part of the American citizen's life." *Rushing*, 71 A.3d at 955. And like the pen register information there, real-time cellular location information exposes to government eyes a wide array of private information. For one, tracking cell phones will "invariably locate people inside private dwellings where their expectation of privacy is at its highest" under Article I, Section 8. *Id.* at 961. Further, like bank records (which have been protected under the State Constitution since 1979), the details of a person's life reflected by their cell phone's comings and goings over time "provides a virtual current biography" that, if not constitutionally protected, "opens the door to a vast and unlimited range of very real abuses of police power." *DeJohn*, 403 A.2d at 1289–90 (quoting *Burrows v.*

Super. Ct. of San Bernardino Cty., 529 P.2d 590, 596 (Cal. 1974)). Indeed, "[t]he ability of law enforcement to pinpoint any cell phone user's location at any moment would intrude on privacy in the same way as allowing police to listen in on an ongoing phone call or to peruse a text message conversation." *Muhammad*, 451 P.3d at 1070; *cf. Commonwealth v. McCoy*, 275 A.2d 28, 31 (Pa. 1971) (noting "concern with the erosion of individual privacy" threatened by wiretapping the contents of phone calls). Thus, "under the Pennsylvania Constitution police were required to make a showing of probable cause in order to obtain real time cell site information data of Appellant's cell phone." *Rushing*, 71 A.3d at 963.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to hold that warrantless real-time tracking of Mr. Pacheco's cell phone constituted a search under the Fourth Amendment and under Article 1, Section 8 of the Pennsylvania Constitution.

September 21, 2020

Respectfully submitted,

/s/ *Andrew Christy*

Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union
of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19102

(215) 592-1513 x138
achristy@aclupa.org
Counsel for Amici Curiae

On the Brief:

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

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758

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

CERTIFICATE OF COMPLIANCE WITH WORD LIMIT

I certify pursuant to Pa.R.A.Ps. 531 and 2135 that this brief does not exceed 7,000 words.

CERTIFICATE OF COMPLIANCE

I certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was served upon the parties at the addresses and in the manner listed below:

Via PACFile

Brooks Thomas Thompson
John I. McMahon, Jr
McMahon, Lentz & Thompson
21 W Airy St.
Norristown, PA 19401

Jerome Michael Brown
Eight Penn Center
1628 JFK Boulevard, Suite 1000
Philadelphia, PA 19103

Kevin R. Steele
Robert Martin Falin
Montgomery County District Attorney's Office
PO Box 311
Norristown, PA 19404-0311

/s/ *Andrew Christy*

Dated: September 21, 2020 Andrew Christy