IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

No. 45 MAP 2020

COMMONWEALTH OF PENNSYLVANIA

Appellee,

v.

ALKIOHN DUNKINS

Appellant.

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA, AND THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT ALKIOHN DUNKINS

Appeal from the order of the Superior Court dated February 12, 2020, No. 1003 EDA 2019, affirming the Judgment of Sentence of the Northampton County Court of Common Pleas, Criminal Division, dated January 4, 2019 at No. CP-48-CR-1577-2017

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

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, and the **ACLU of Pennsylvania** is a state affiliate. 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 works to protect free speech and privacy rights in the online and digital world. EFF served as amicus in numerous cases addressing Fourth Amendment protections for cell phone location information, including *Carpenter*.[1]

SUMMARY OF ARGUMENT

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). That is because the Internet plays an essential role in modern life. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735–36 (2017); *J.I. v. N.J. State Parole Bd.*, 155 A.3d 1008, 1012 (N.J. 2017). But accessing the Internet often requires using Wi-Fi, especially for students, low-income people, and people traveling away from

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

home. Wi-Fi use generates precise location data that can reveal the most intimate details of people's lives, as well as identify all the people present in a particular space at a particular time, as campus police did in this case.

That capability poses a grave threat to privacy and constitutes a sweeping expansion of government power. Just as with the historical cell phone location records at issue in *Carpenter*, there is a reasonable expectation of privacy in the Wi-Fi–derived location tracking data in this case. A private terms of service or acceptable use policy does not diminish this privacy expectation as to law enforcement. Consequently, law enforcement's acquisition of Wi-Fi–derived location information without a warrant violates the Fourth Amendment.[2] .

In this case, after two men robbed a Moravian College student's dorm room in the early morning hours of February 2, 2017, police obtained logs showing all devices that were connected to the residence hall's Wi-Fi access points during the relevant time period (between 1:30 a.m. and 2:30 a.m.).[3] Officers cross-referenced those logs with other records to identify three devices present in the residence hall that night that belonged to non-resident students. Of those three devices, two

---

[2] Wi-Fi–derived location data is also protected under Article I, Section 8 of the State Constitution, which protects privacy to an even greater degree than does the Fourth Amendment. P.A. Const. art. I, § 8.

[3] Wi-Fi is a radio-based networking technology that is typically used to connect portable devices, such as phones, tablets, and laptops, to the Internet. *See* Eric Escobar, *How Does Wi-Fi Work?*, Sci. Am. (July 15, 2015), https://www.scientificamerican.com/article/how-does-wi-fi-work/.

belonged to women. The only account belonging to a non-resident male was that of Mr. Dunkins. (R.R. 410–411a.) Officers then searched the logs of every Wi-Fi access point on campus to compile a record of Mr. Dunkins' movements over a five-hour period on the night of the robbery. (R.R. 62a.)

This Court should hold that campus police violated the Fourth Amendment when they warrantlessly obtained Wi-Fi location data placing Mr. Dunkins and other students in the Hassler dorm rooms that evening and when they tracked Mr. Dunkins' movements over a five-hour period. Moreover, although police made no attempt to even try to get a warrant in this case, any attempt to do so as to the first search (locating all students in the residence hall) would have implicated serious questions underlying the Fourth Amendment's rejection of general warrants and overbroad searches. Because police infringed on reasonable expectations of privacy, the evidence should be suppressed.

ARGUMENT

I. Wi-Fi–Derived Location Information Can Provide Law Enforcement with Precise and Voluminous User Location Data.

Because of the way that devices like cell phones, tablets, and laptops connect to wireless Internet networks, those devices generate precise information about users' current or historical locations. When these kinds of Wi-Fi networks are operated by entities like colleges, businesses, or city governments, those entities thereby obtain a log of location information about any user accessing them.

This information, often timestamped down to the second, provides a detailed picture of where a given Wi-Fi user has been in space and time.

A. Wi-Fi Networks Collect User Devices' Information as They Connect to the Internet.

An overwhelming majority of Americans now own smartphones and connect these phones to Wi-Fi networks in their homes, offices, and in public spaces to browse the Web, connect with friends over social media, play games, and send text messages or e-mail.[4] Wi-Fi networks use radio technology to connect user devices like cell phones, tablets, and laptops to physical devices called Wi-Fi "access points," which in turn connect to the Internet.[5] The radio contained within each phone, laptop, or other device is manufactured with a unique identifier called a "MAC address," which is a code made up of letters and numbers.[6] Access points use these unique codes to identify and log information about which devices are communicating with them at any given time.[7]

B. Wi-Fi Networks Can Log Device Locations as Their Users Move Throughout Physical Space.

---

[4] *See* Pew Res. Ctr., *Mobile Fact Sheet* (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[5] *See* Wikipedia, *Wireless Access Point*, https://en.wikipedia.org/wiki/Wireless_access_point.

[6] *See* Wikipedia, *MAC Address*, https://en.wikipedia.org/wiki/MAC_address.

[7] *See Monitoring Wireless Networks through Log Checking*, Who's On My WiFi, https://whoisonmywifi.com/more-info/additional-info/monitoring-a-wireless-network/log-checking/. In this case, the Wi-Fi network logs provided to police identified devices by users' unique usernames instead of the devices' underlying MAC addresses. *See* Trial Ex. 2, at 8–12.

Wi-Fi networks can be used to track users' location and movements through physical space. Because network administrators know where access points are physically located within a Wi-Fi network, and because networks log the exact time and date each device connected to each access point, administrators also know that the devices connecting to those access points are in the nearby vicinity and know when they connected.

While a home network may rely on only a single access point, a larger network—covering an office building, college campus, neighborhood, or even an entire city—must deploy multiple access points to ensure users' seamless connections to the Internet. That is because the typical range of a Wi-Fi access point is approximately a few hundred feet, under perfect conditions.[8] Additional access points are necessary in larger geographic areas, as well as in dense indoor areas, like offices or dormitories, because heavy materials like concrete, cinder block, and brick can block Wi-Fi radio waves.[9] Further, each access point can only

[8] *See What is the Typical Range of a Wireless LAN?*, SpeedGuide.net, https://www.speedguide.net/faq/what-is-the-typical-range-of-a-wireless-lan-330.

[9] *See* Jorunn D. Newth, *Which Building Materials Can Block Wi-Fi Signals?*, Eye Networks, https://eyenetworks.no/en/wifi-signal-loss-by-material/; *see also* R.R. 401a.

support a limited number of devices, so a network supporting a large number of devices, as in a college dorm, requires many access points to avoid congestion.[10]

The more access points a network has within its geographic area, the more detailed and specific the location information it can generate. In this case, Moravian densely blanketed the campus, an area spanning about six blocks, with over 1,100 access points to ensure students receive signal anywhere on campus. (R.R. 51a.) The College placed access points in classrooms and dining halls, as well as outside buildings—basically, "anywhere a human being who wants to access the wireless [I]nternet will be," (R.R. 54a), including up to eighty to ninety access points each in certain residence halls, yielding one access point for approximately every other dorm room. (R.R. 73a–74a.)

When a device is connected to a Wi-Fi network that uses multiple access points, that device will automatically "roam" between access points, communicating with whichever access point has better signal strength or less interference at any given point in time. Once the device connects to the Wi-Fi network for the first time, switching happens automatically. This happens even when a device is not actively in use, as devices continuously maintain an association with the closest Wi-Fi access point. If a user moves from the first floor

[10] *See Wireless Network Capacity*, Actiontec, https://www.actiontec.com/wifihelp/wireless-network-capacityhow-many-devices-can-connect-wifi-network/.

to the second floor of a building, for example, their phone will likely switch from communicating with an access point on the first floor to communicating with one on the second floor. The Wi-Fi network logs each of these connections, allowing administrators to track when the device was in the building and where it travelled while it was there.[11]

Once a device connects to a Wi-Fi network, a user's location information is collected automatically. On many such systems, including Moravian's, users need only log in once for their phones to connect to the network every time they are in range, in perpetuity. This continuous data collection occurs even if a user leaves the coverage network and returns later; once connected, a user's device automatically re-joins the Wi-Fi network without having to log in, view terms of service, or accept network terms. (R.R. 53a, 404a.) This allows a network like Moravian's to track a student's location and movement across campus over an entire day or even over their entire tenure at the College. (R.R. 70a.) In an area with complete Wi-Fi coverage, like Moravian, the only time that records of users' location will not be produced is when the user deliberately turns off Wi-Fi.[12]

---

[11] Location tracking is also possible across networks. Investigators would just need to obtain access point logs from each network administrator.

[12] Many devices automatically turn Wi-Fi back on, even if a user has turned it off. *See, e.g., Use Bluetooth and Wi-Fi in Control Center,* Apple, https://support.apple.com/en-us/HT208086 (noting iPhones and iPads will automatically turn on again if "[y]ou walk or drive to a new location" or "[i]t's 5 AM local time.")

C. Wi-Fi–Derived Location Information Can Tie Users' Devices to Users' Identities.

It is a short step from obtaining location information about devices using the network to identifying the device user. Some Wi-Fi networks allow users to connect without registering their identifying information. But today many require user authentication, meaning that users must create a username and password, or otherwise authenticate their devices with the network.[13] When users connect to "authenticated" Wi-Fi networks, such as Moravian's, the network data can connect a particular *device* to a particular *person*.

Many different entities use authenticated Wi-Fi networks, ranging from hotels (where users must enter their room numbers to connect) to municipal Wi-Fi networks like New York City's LinkNYC Program (which generally require users to enter their email addresses when they first connect). Colleges and universities, like Moravian, often host authenticated networks that require students, faculty, and staff to enter their college-provided username and password. (*See* R.R. 51a–52a, 404a.) Administrators of authenticated networks are not only able to identify which devices are connected to Wi-Fi, but also whom those devices belong to based on their login information.

---

[13] *See* Norton, *The Dos and Don'ts of Using Public Wi-Fi*, https://us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html.

In turn, reviewing multiple access point logs can provide a detailed picture of a particular user's location as they move through physical space. Such review can also reveal everyone who was in a particular vicinity at a particular point in time. (*See* R.R. 409a–410a.)

D. Warrantless Law Enforcement Use of Wi-Fi–Derived Location Information Poses Serious Concerns for All Americans.

The implications of a rule permitting warrantless law enforcement access to Wi-Fi–derived location information stretch well beyond entities like Moravian, or even much larger colleges and universities such as University of Pennsylvania (26,675 students)[14] and Penn State (96,408 students).[15] Many municipalities offer free Wi-Fi, including as part of transit systems like SEPTA;[16] via kiosks, community centers, or public libraries, as in Philadelphia;[17] or in city parks as in Pittsburgh.[18] Cities across the country, ranging from Boston to El Paso, have built free municipal Wi-Fi networks spanning significant portions of their geographic

---

[14] *Facts*, University of Pennsylvania, https://home.www.upenn.edu/about/facts.

[15] *At A Glance*, Pennsylvania State University, https://stats.psu.edu/.

[16] *See Wireless Internet Hotspots*, SEPTA, https://www.septa.org/events/wifi.html.

[17] *See* Victor Fiorillo, *Here's Where to Get Free Wi-Fi in Philly*, Philadelphia (Feb. 18, 2020), https://www.phillymag.com/news/2020/02/18/free-wifi-in-philly/.

[18] *See* Comcast W. Pa., *Comcast Installs WiFi Hotspots at Nine City of Pittsburgh Parks*, https://westernpa.comcast.com/2017/07/30/comcast-installs-wifi-hotspots-at-nine-city-of-pittsburgh-parks/.

territory.[19] A host of private entities have deployed Wi-Fi networks throughout cities. Comcast, for example, has deployed "millions of hotspots."[20] Alone or in conjunction with other networks, the widespread deployment of Wi-Fi networks constitutes a relatively ubiquitous and comprehensive location surveillance tool.

While the tracking enabled by these networks is troubling for all segments of society, it will particularly affect poor people and people of color, who often rely on Wi-Fi networks outside their homes for connectivity. Cities offer municipal Wi-Fi networks with the goal of alleviating disparities in Internet access. When New York City rolled out the LinkNYC Program,[21] for example, a city official stated: "With this hotspot, this city takes an important step toward a fairer distribution of broadband service. We know that low income New Yorkers, particularly African American and Latino residents, rely on their smartphones to get online."[22] Philadelphia, which has one of the lowest rates of broadband access of any large city in the United States, also hopes its Link program will help to shrink the digital

---

[19] *See* Wikipedia, *Municipal Wireless Network*, https://en.wikipedia.org/wiki/Municipal_wireless_network#United_States.

[20] Xfinity WiFi, https://wifi.xfinity.com/.

[21] *See* LinkNYC, https://www.link.nyc.

[22] NYC.gov, *Mayor de Blasio Announces Public Launch of LinkNYC Program, Largest and Fastest Free Municipal Wi-Fi Network in the World* (Feb. 18, 2016), https://www1.nyc.gov/office-of-the-mayor/news/184-16/mayor-de-blasio-public-launch-linknyc-program-largest-fastest-free-municipal#/0.

divide.[23] Those who rely on public Wi-Fi networks for connectivity are at even greater risk of surveillance because they may have few other options for Internet connectivity.

II. Warrantless Acquisition of Wi-Fi–Derived Location Information Violates the Fourth Amendment.

The Superior Court erred when it held that Mr. Dunkins had no expectation of privacy in his cell phone location information recorded by the college's Wi-Fi network. *Commonwealth v. Dunkins*, 229 A.3d 622, 629 (Pa. Super. Ct. 2020). Contrary to the lower court's view, law enforcement access to Wi-Fi location information without a warrant infringes on individuals' expectations of privacy for much the same reason that the GPS monitoring of vehicles at issue in *United States v. Jones*, 565 U.S. 400 (2012), and the cell site location information in *Carpenter* do. The data facilitates detailed, pervasive, cheap, and efficient tracking of millions of Americans in previously impossible ways. *See Carpenter*, 138 S. Ct. at 2217–18; *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in judgment); *id.* at 415–16 (Sotomayor, J., concurring).

---

[23] *See* Bob Fernandez, *In Comcast's Hometown, the Chasm Between Internet Haves and Have-Nots Looks Intractable, New Census Data Shows*, Phila. Inquirer (Dec. 10, 2018), https://www.inquirer.com/news/comcast-digital-internet-access-philly-poor-people-20181210.html; Julie Zeglen, *Philly's Digital Divide Is Growing, But At Least We Got Some Free Wi-Fi Kiosks*, Generocity (Dec. 11, 2018), https://generocity.org/philly/2018/12/11/phillys-digital-divide-is-growing-but-at-least-we-got-some-free-wi-fi-kiosks/.

A. The Data Is Detailed and Pervasive.

As the U.S. Supreme Court stated in *Carpenter*, "like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." 138 S. Ct. at 2216. As described above, Wi-Fi–derived location data shares these characteristics. Because Wi-Fi transmitters have short broadcast ranges—from just fifteen to twenty feet inside of buildings, to approximately 200 feet in unobstructed areas outside (R.R. 403a, 418a)—Wi-Fi location data pinpoints individuals' locations with greater precision than the cell phone data at issue in *Carpenter* or even the GPS tracker in *Jones*. *See Carpenter*, 138 S. Ct. at 2218 (CSLI accurate to within one-eighth to four square miles); *Jones*, 565 U.S. at 403 (GPS device accurate to within 50–100 feet).

Furthermore, Wi-Fi location data allows the government to track people inside of constitutionally protected spaces that reveal private information about their lives. In this case, for example, Wi-Fi access points blanket the Moravian campus, "inside, outside, in the dormitories, in the bedrooms, in the classrooms," and everywhere else. (R.R. 400a.) Wi-Fi location information reveals people's presence in homes, offices, houses of worship, medical facilities, 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.

Kyllo v. United States, 533 U.S. 27, 40 (2001); *United States v. Karo*, 468 U.S. 705, 716 (1984).

In this regard, the Superior Court was wrong to hold that the Fourth Amendment does not apply because it merely reveals an individual's location while "present on the Moravian campus." *Dunkins*, 229 A.3d at 629. While it is true that a college campus is a defined geographic area, that does not make an individual's movements within that area any less private from the government than the movements at issue in *Carpenter*. At a residential college like Moravian, most students will spend most of their time on campus.[24] Wi-Fi location data will reveal the full spectrum of those students' "privacies of life," *Carpenter*, 138 S. Ct. at 2217 (citations omitted), from where they sleep at night, to when they visit the campus health or counseling centers, to their patterns of exercise, socializing, attending meetings of activist or political organizations, and more. Other Wi-Fi networks log similarly rich chronicles of peoples' locations and movements, including their movements around a particular neighborhood or an entire city, and raise equivalent concerns. *Supra* Part I.[25] Thus, "[m]apping a cell phone's location

---

[24] *See Residence Life and Housing*, Moravian College, https://www.moravian.edu/rlh/on-campus/on-campus-overview ("All full-time undergraduate students are guaranteed on-campus housing. Full-time undergraduate students whose permanent address is more than 50 miles from the College are required to live on campus.").

[25] Additionally, law enforcement could access and aggregate logs from multiple Wi-Fi networks looking for the handset's unique identifier and thereby expand the area of surveillance to anywhere that Wi-Fi reaches, regardless of whether it is a single network, or many.

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)).

B. The Data Collection Is Nearly Ubiquitous.

An equally important factor in *Carpenter* was the recognition that cell phone location information allows the government to access the patterns of movement of essentially any person at any time. "[T]his newfound tracking capacity runs against everyone," the Court wrote, and "[o]nly the few without cell phones could escape this tireless and absolute surveillance." 138 S. Ct. at 2218.

The same is true of Wi-Fi location information. Both cell phones and Internet access are "indispensable to participation in modern society," *Carpenter*, 138 S. Ct. at 2220, and Wi-Fi use is both pervasive and essential. In this case, Moravian's students, faculty, and staff, have their location information logged as they move around campus. Moravian is far from unique in this regard. Students at colleges and universities across the country, not to mention residents of the numerous cities with municipal and commercial Wi-Fi networks, are subject to such tracking as well.

C. The Data Permits Retrospective Searches.

The third factor that led the Court in *Carpenter* to distinguish CSLI from traditional law enforcement surveillance was "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable." *Id.* at 2218. As the Court explained, CSLI is akin to a time machine that allows law enforcement to look at a suspect's past movements, something that would be physically impossible without the aid of technology: "In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers." *Id.* Wi-Fi–derived location information provides equivalent capabilities.

D. Wi-Fi–Derived Location Tracking Grants Police an Unprecedented Power.

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). As with cell site location information, acquiring Wi-Fi location information is "remarkably easy, cheap, and efficient compared to traditional investigative tools," violating people's expectations of privacy and demanding Fourth Amendment regulation. *Carpenter*, 138 S. Ct. at 2218.

* * * * *

The confluence of these factors—detailed, indiscriminate, and pervasive location data collection enabling highly efficient retrospective searches—explains why the Superior Court was wrong to conclude that a search of Wi-Fi location data "functions similarly to a security camera." *Dunkins*, 229 A.3d at 629. At the time of the search, the Moravian campus's approximately 1,100 Wi-Fi access points provided "curb-to-curb wireless, meaning that if you're on Moravian College property, you have access to [the] network," regardless of whether you are outside in a public area or inside in your dorm room. (R.R. 400a.) In contrast, security cameras are unlikely to record presence "in classrooms, in dining halls," and could never reach into private dorm rooms and bathrooms. (R.R. 54a.) Moreover, a security camera cannot, "[w]ith just the click of a button," *Carpenter*, 138 S. Ct. at 2218, call up a comprehensive list of every person who was near it at a particular time, unhindered by masks, hats, or darkness, much less instantly reconstruct a person's movements across campus, well beyond visual range.

These factors also explain why even acquisition of shorter-term Wi-Fi location information is a Fourth Amendment search. Fourth Amendment protections apply regardless of the length of time a person is electronically located and tracked because even short-term surveillance can reveal presence in constitutionally-protected spaces.[26] Moreover, even if some types of less-precise location information were to be protected only over longer periods, the precision of Wi-Fi–derived location information, placing people within a specific building or even a particular room, 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, 1199

---

[26] In holding that collecting seven days of location data was a search, the *Carpenter* Court did not suggest that collection of location data over a shorter period would evade Fourth Amendment protection. Before and after *Carpenter*, courts have held that much shorter collection of location information deserves protection. *See, e.g.*, *State v. Muhammad*, 451 P.3d 1060, 1072–73 (Wash. 2019) (holding that a single ping of cell-phone location information is a search requiring a warrant); *Commonwealth v. Almonor*, 120 N.E.3d 1183, 1197 (Mass. 2019) (same); *Tracey v. State*, 152 So. 3d 504, 520 (Fla. 2014) (refusing to base Fourth Amendment protection of real-time CSLI on the length of the time the cell phone is monitored); *see also Karo*, 468 U.S. at 715–716 (learning information about presence inside a home using a radio beeper is a search).

Those rulings make sense. As Justice Sotomayor pointed out in *Jones*, "even short-term monitoring" of location using advanced technologies implicates society's reasonable expectations of privacy by threatening to reveal "a wealth of detail about . . . familial, political, professional, religious, and sexual associations" and thereby "alter[ing] the relationship between citizen and government in a way that is inimical to democratic society." 565 U.S. at 415–16 (Sotomayor, J., concurring) (citation omitted).

(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.").

The power to "travel back in time to retrace a person's whereabouts" only enhances that threat to privacy. *Carpenter*, 138 S. Ct. at 2218. Prior to the digital age, the government would rarely have been able to perfectly reconstruct a person's past movements over even a short period, or even to reliably identify their location at one specified point in time. Today, even short-term aggregations of Wi-Fi–derived location information—such as the five hours here—instantaneously "expos[e] a cell phone user's attendance at a location a person would reasonably expect to be private," *Muhammad*, 451 P.3d at 1070 (citation omitted). Therefore, it makes little sense to draw an "arbitrary" line based on the extent of location information obtained. *Muhammad*, 451 P.3d at 1072–73.

For these reasons, the campus police required a warrant to obtain five hours of Wi-Fi–derived location data revealing Appellant's movements around campus.

III. Using Wi-Fi Access Point Data to Identify All People in a Particular Location Is Unconstitutional.

Likewise, law enforcement access to a list of all people whose devices were in range of one or more Wi-Fi access points during a specified time period is a Fourth Amendment search. This tool enables an unprecedented and chilling police power; identification of essentially all people in a particular place at a particular

time. This law enforcement capability upends the traditional balance of power between the people and the police.

The Superior Court analogized the police search to identify individuals present in the dorm to a cellular service "tower dump." "Tower dump" refers to "a download of information on all the devices that connected to a particular cell site during a particular interval." *Dunkins*, 229 A.3d at 629 (citing *Carpenter*, 138 S. Ct. at 2220). The court concluded that because *Carpenter* reserved decision on the permissibility of tower dumps, the Fourth Amendment was not implicated here. *Id.* at 629. Of course, the *Carpenter* Court did not address the constitutionality of CSLI tower dumps because it could not have done so on the facts before it, not because the Court meant to signal a premature answer to that question.

This Court need not rule on the constitutionality of tower dumps, because attributes of Wi-Fi–derived location information make clear it is a search lacking the particularity that the Fourth Amendment requires. U.S. Const, amend. IV; *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). In this case, police were able to pinpoint students to within one or two specific dorm rooms. (R.R. 74a, 403a.) *See also supra* Part II (discussing Fourth Amendment protection for information about presence inside constitutionally protected spaces). They learned not only that two women who were not residents of the building were nonetheless present in the wee hours of the morning, but even which rooms they were present in. (*See* Trial Ex. 2,

at 8–12.) That is just one example of how private information can be—and was—discovered in such a search. (R.R. 410–411a.) While looking for the perpetrator, the campus police impinged not only on the privacy of Appellant, but also of innocent third parties like these two women and their hosts. The same investigative technique can reveal everyone present at a political gathering, a mental health center, or an Alcoholics Anonymous meeting. By sweeping in information about a large number of people who could not possibly have had anything to do with the crime under investigation, the search was incompatible with the Fourth Amendment's prohibition on overbroad searches. (*See* Trial Exhibit 2, at 2 (search identified about thirty-eight students present in the dorm at that time).)

Preventing overbroad searches by government agents was a central concern motivating the framers of the Fourth Amendment. In the American colonies, British agents used general warrants and "writs of assistance" to conduct broad searches for smuggled goods, limited only by the agents' own discretion. *See Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley v. California*, 573 U.S. 373, 403 (2014).

A search of the Wi-Fi location information of every student in a residence hall—information that may be precise enough to place individuals in particular dorm rooms—in the hope that it will turn up the identity of one criminal suspect, is akin to a search of every house in an area of a town—simply on the chance that the suspect might be located inside one. Even when targeted surveillance using modern technologies could be reasonable under the Fourth Amendment, dragnet collection of many people's private information would not be. *See United States v. Knotts*, 460 U.S. 276, 284 (1983) (comparing use of a beeper, which requires resource-intensive tailing at close range by a human with an analog radio receiver to "dragnet type law enforcement practices," which would raise a distinct constitutional question). What's more, the ability to *retrospectively* call up a list of everyone who was in a particular building—or even a room of that building—at a moment in the past imperils privacy and threatens to chill freedom of association in ways the Founders could not have imagined.

Recently, courts have rejected the government's attempts to engage in similar types of retrospective digital dragnet searches. In recent years, police have begun making "geofence" requests to Google, asking the company to identify all

users whose smartphones were in a specific area at a particular time.[27] Even with a warrant, two federal magistrate judges recently held these searches to be overbroad general warrants. *In re Search of: Info. Stored at Premises Controlled by Google*, No. 20 M 392, __ F. Supp. 3d __, 2020 WL 4931052 (N.D. Ill. Aug. 24, 2020) [hereinafter *Fuentes Geofence Opinion*]; *In re Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020) (slip op.). This is because, by sweeping in information about many bystanders simply by virtue of their unwitting proximity to the scene of an alleged crime, the searches lack particularity and individualized suspicion as required by the Fourth Amendment. *Fuentes Geofence Opinion*, 2020 WL 4931052, at *14 (citing *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979)). Like overbroad demands for Google users' location information, the overbroad Wi-Fi–derived location search in this case constitutes a "general, exploratory rummaging" intolerable under the Fourth Amendment. *Fuentes Geofence Opinion*, 2020 WL 4931052, at *7 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

Because police made no attempt to even try to get a warrant in this case, the search was clearly unconstitutional. But in deciding this case, the Court should also

[27] *See* Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

bear in mind that any attempt to secure judicial authorization for such an overbroad search would run up against the Fourth Amendment's prohibition on general warrants.

IV. The Third-Party Doctrine Does Not Vitiate the Privacy Rights at Issue in this Case.

In *Carpenter*, the Supreme Court held that the mere fact that records are held by a third party does not vitiate an individual's reasonable expectation of privacy under the Fourth Amendment. 138 S. Ct. at 2220. Instead, the Court explained, the cases on which the third-party doctrine is based—*United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979)—require a dual inquiry into "the nature of the particular documents sought" and whether they were voluntarily exposed. 138 S. Ct. at 2219–20. Here, both factors favor the conclusion that the third-party doctrine does not apply.[28]

First, Wi-Fi–derived location information is highly sensitive, revealing numerous privacies of life. *Supra* Parts II–III.

Second, it is not voluntarily exposed. As the Supreme Court explained in *Carpenter*, "cell phone location information is not truly 'shared' as one normally

[28] In addition, this Court has long rejected the third-party doctrine as "a dangerous precedent, with great potential for abuse" when interpreting the state constitutional protection against unreasonable searches and seizures in Article I, Section 8. *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979).

understands the term," both because carrying a cell phone is "indispensable to participation in modern society," and because once a person has an operational cell phone, it automatically and inescapably generates location data. 138 S. Ct. at 2220.

Wi-Fi is indispensable in American society, and on the Moravian campus. "Today, the Internet plays an essential role in the daily lives of most people—in how they communicate, access news, purchase goods, seek employment, perform their jobs, enjoy entertainment, and function in countless other ways." *J.I. v. N.J. State Parole Bd.*, 155 A.3d at 1012. Many people—disproportionately young, poor, or people of color—rely out of necessity on Wi-Fi connections to access the Internet and use apps on their phones. *Supra* I.D. At Moravian, students must use the network—hardwired or Wi-Fi—for access not only to the Internet, but also to the school's online resources.[29]

Further, use of Wi-Fi automatically and inescapably generates location data. *Supra* Part II.B; (R.R. 53a.) Both a cellular telephone connection and a Wi-Fi network require the user to initially configure their phone to communicate with the network, and thereafter the phone automatically connects to cellular towers or Wi-Fi access points in range, regardless of whether the person is using the device.[30]

---

[29] *Welcome to AMOS,* Access Moravian Online Servs., https://amos.moravian.edu/ICS.

[30] *See, e.g., First Use Configuration and Device Activation: iPhone*, T-Mobile, https://www.t-mobile.com/support/devices/apple/first-use-configuration-and-device-activation-iphone ("Before

(R.R. 61a, 76–77a.) Just as in *Carpenter*, Wi-Fi "logs a [location] record by dint of its operation, without any affirmative act on the part of the user beyond powering up." 138 S. Ct. at 2220. "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id.*

Like the CSLI in *Carpenter*, Wi-Fi–derived location information is in no meaningful sense voluntarily shared.

V. Moravian's Student Handbook Does Not Defeat Appellant's Reasonable Expectation of Privacy in His Location Data.

The Superior Court was wrong to conclude that a provision in the Moravian Student Handbook eliminated Appellant's reasonable expectation of privacy in his Wi-Fi–derived location information. *Dunkins*, 229 A.3d at 626.

Upon enrollment, students are generally required to sign a document stating that they have been given a copy of the Moravian Student Handbook. (R.R. 36a.)[31] The Handbook includes policies about parking, financial aid, and housing, the student code of conduct, the academic code of conduct, and more.[32] Part of this document advises individuals that the college may collect and disclose all Internet data composed, transmitted, or received through the campus computer system and

---

the iPhone can be used, it must first be activated and configured to work on the T-Mobile network.").

[31] The record contains no evidence that Appellant signed the Handbook.

[32] *Student Handbook*, Moravian College, https://www.moravian.edu/handbook.

its network connections. *Dunkins*, 229 A.3d at 626. The Handbook does not mention any kind of location tracking. Despite that, the Superior Court held that pursuant to the Handbook, Appellant forfeited any expectation of privacy in data his phone generated, including location data, and had voluntarily consented to its disclosure to law enforcement. *Id.*

Privacy policies, terms of service (TOS), and acceptable use policies (AUP) such as the one included in the computing resources section of the College Handbook do not determine an individual's Fourth Amendment rights to be free of unreasonable *government* searches and seizures. Service providers regularly develop non-negotiable statements of policy to advance their private interests. Communications services almost always claim the right to conduct private searches for business reasons, including identifying and stopping unlawful abuse of the service. But the fact that a private entity reserves the right to review data on its network or interdict illegal activity does not empower *the police* to collect that information without a warrant. Were that true, *Carpenter* would have been decided differently.

In *Carpenter*, the Supreme Court made clear that one's reasonable expectation of privacy in information as against the police is not automatically defeated merely because a third party has access to or control over that information. 138 S. Ct. at 2219–20. *Carpenter* would have been decided the other

way if cell phone users' reasonable expectation of privacy could be defeated by a private notice. Every cellular service provider (including Sprint and MetroPCS, which Mr. Carpenter's phone used) has a terms-of-service agreement that allows provider access to enforce the law.[33] Every Justice of the Supreme Court in that case also suggested that the Fourth Amendment protects the content of digital documents stored with third parties. *See Carpenter*, 138 S. Ct. 2206, 2222 (majority op.); *id.* at 2230 (Kennedy, J., dissenting); *id.* at 2262–63, 2269 (Gorsuch, J., dissenting). This is true even though—as with cellular service providers—essentially every Internet service comes with a privacy policy, TOS, or AUP that permits the provider some access to stored files and accompanying transactional data, including for law enforcement purposes.[34]

Terms of service and AUPs, with their reservations of rights, are almost never negotiated. These policies are often buried on a website or in an app, where the user has no choice but to "agree" by clicking a box. Here, in the first days of school, and presumably along with housing assignments, cafeteria hours, and

---

[33] *See Sprint/T-Mobile Privacy Policy*, T-Mobile, https://www.t-mobile.com/privacy-center/our-practices/privacy-policy ("We may disclose personal data to third parties involved in legal process or protection matters, including government authorities, where we believe that access, use, preservation or disclosure of such information is reasonably necessary.").

[34] *See, e.g.*, *Privacy Policy*, Google, https://policies.google.com/privacy (Company will share personal information upon a good-faith belief that sharing is reasonably necessary to comply with the law, with enforceable governmental requests, to detect fraud, protect Google's rights and property, and more.); Microsoft Privacy Policy, https://privacy.microsoft.com/en-US/privacystatement (similar).

campus maps, students receive a copy of the multi-policy Handbook and are told they must sign a document indicating that they've received and understood the terms. They likely sign before even reading the document. Students have no choice; they've already enrolled, paid, and shown up.

The U.S. Supreme Court recently rejected the argument that Fourth Amendment rights can be determined by private form contracts. In *Byrd v. United States*, 138 S. Ct. 1518 (2018), the police stopped and searched a rental car driven by someone who was not on the rental agreement but was given permission to drive by the renter. The Court held that drivers have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement. *Id.* at 1529. Car-rental agreements, wrote the Court, are filled with long lists of restrictions that have nothing to do with a driver's reasonable expectation of privacy in the rental car. Even a serious violation of the rental agreement has no impact on expectation of privacy. Rental agreements, like terms of service, "concern risk allocation between private parties . . . . But that risk allocation has little to do with whether one would have a reasonable expectation of privacy in the rental car if, for example, he or she otherwise has lawful possession of and control over the car." *Id.* Since the defendant in *Byrd* was lawfully in possession of the car, despite the fact that he was violating a private agreement, he had an expectation of privacy.

The specific wording of the Handbook should not define the scope of Moravian students' expectations of privacy. Basing constitutional rights on the linguistic details of a website or Handbook notice would lead to a difficult-to-administer patchwork. For example, even in *Smith v. Maryland*—one of the cases that spawned the modern third-party doctrine—the Court noted, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." 442 U.S. at 745. And in *United States v. Owens*, the Tenth Circuit did not let a motel's private terms govern the lodger's expectation of privacy, noting, "[a]ll motel guests cannot be expected to be familiar with the detailed internal policies and bookkeeping procedures of the inns where they lodge." 782 F.2d 146, 150 (10th Cir. 1986).

Appellant therefore retained his expectations of privacy in his location data. The school might permissibly access that data for its own administrative purposes (network diagnostics, for example). But when, as here, the campus police are investigating criminal activity and direct college personnel to search for and disclose sensitive information, that requires at least a search warrant.

The cases cited by the Superior Court in reaching its holding are inapposite or distinguishable. Both *Commonwealth v. Sodomsky*, 939 A.2d 363, 369 (Pa. Super. Ct. 2007), and *United States v. Adkinson*, 916 F.3d 605 (7th Cir. 2019),

involved private, not law enforcement searches. *See United States v. Jacobsen*, 466 U.S. 109, 115–117 (1984) (law enforcement may replicate private party search that uncovers evidence of a crime, but may not exceed scope of private search). *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), involved a government employer's policy on employee use of employer-provided computers and network access. *Medlock v. Trustees of Indiana University* involved a public university conducting a *regulatory*, not a law enforcement, search. 738 F.3d 867, 872–73 (7th Cir. 2013). Here, in contrast, the search was conducted from the outset by campus police for law enforcement purposes. None of these cases justify warrantless law enforcement searches of college students' or members of the public's private data or movements.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to hold that warrantless acquisition of Wi-Fi–derived location information violates the Fourth Amendment.

September 28, 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

[*] Counsel thank law student Rachel D. Maremont, who contributed to preparation of this Brief.

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

Michael Jay Diamondstein
Stephanie Renee Esrig
Michael J. Diamondstein PC
Two Penn Center, Suite 900
1500 JFK Boulevard
Philadelphia, PA 19102

Rebecca J. Kulik
Terence Patrick Houck
Katharine R. Kurnas
Northampton County District Attorney's Office
669 Washington Street
Easton, PA 18042-7490

/s/ *Andrew Christy*

Dated: September 28, 2020 Andrew Christy