COMMONWEALTH OF MASSACHUSETTS

Supreme Judicial Court

No. SJC-12938

Commonwealth of Massachusetts

Appellant

v.

Dondre Snow,

Defendant-Appellee.

ON APPEAL FROM A JUDGMENT OF
THE SUFFOLK SUPERIOR COURT

BRIEF AMICI CURIAE OF THE AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC. AND THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF THE APPELLEE

Jennifer Lynch (CA 240701)
Andrew Crocker (CA 291596)
Mark Rumold (CA 279060)
Hannah Zhao (NY 5468673)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org

Matthew R. Segal (BBO #654489)
Jessie J. Rossman (BBO 670685)
Jessica J. Lewis (BBO #704229)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MASSACHUSETTS, INC.
211 Congress Street
Boston, MA 02110
(617) 482-3170
jrossman@aclum.org

AUGUST 28, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES..... 4

CORPORATE DISCLOSURE STATEMENTS..... 7

STATEMENT OF INTERESTS OF AMICI..... 9

INTRODUCTION..... 10

STATEMENTS OF THE FACTS AND CASE..... 12

SUMMARY OF ARGUMENT..... 16

ARGUMENT..... 17

I. Cell phones are ubiquitous features of everyday life, with the capacity to store vast amounts of personal data. 17

A. Cell phones contain a vast amount of private data about their users..... 18

B. Cell phones are unique tools for exercising constitutional rights and conducting private communications..... 20

II. This Court has determined that the vast storage and communications capacities of cell phones cannot automatically establish probable cause to search and seize a person’s cell phone. 23

A. The Supreme Court has limited searches of cell phones incident to arrest because they contain vast, private, and sensitive information..... 23

B. *White* requires probable cause to believe that particularized evidence related to the crime under investigation exists on the cell phone.. 25

III. This Court should reaffirm *White*’s holding that police need particularized evidence connecting the cell phone to be searched with the crime under investigation. 27

A. Mere presence and use of a cell phone at the scene of an arrest fails to establish probable cause to search the device..... 27

B. The Commonwealth’s inability to identify a timeframe or location for any alleged evidence on the phone further underscores their lack of probable cause..... 32

C. The Commonwealth’s approach threatens privacy. 34

CONCLUSION..... 37

CERTIFICATE OF COMPLIANCE..... 39

AFFIDAVIT OF SERVICE..... 39

TABLE OF AUTHORITIES

CASES

Buckham v. State,
185 A.3d 1 (Del. 2018) 28, 31

Carpenter v. United States,
138 S. Ct. 2206 (2018) 9

Commonwealth *v. Almonor*,
482 Mass. 35 (2019) 9

Commonwealth v. Arthur,
94 Mass. App. Ct. 161 (2018) 30

Commonwealth v. Augustine,
472 Mass. 448 (2015) 9, 24

Commonwealth v. Broom,
474 Mass. 486 (2016) 30

Commonwealth v. Dorelas,
473 Mass. 496 (2016) 17, 23

Commonwealth v. Evelyn,
SJC-12808 (2020) 9

Commonwealth v. Freiberg,
405 Mass. 282 (1989) 34

Commonwealth v. Goncalves-Mendez,
484 Mass. 80 (2020). 32

Commonwealth v. Holley,
478 Mass. 508 (2017) 29

Commonwealth v. Jordan,
91 Mass. App. Ct. 743 (2017) 29, 31, 32

Commonwealth v. Morin,
478 Mass. 415 (2017) 28, 29

Commonwealth v. Pope,
354 Mass. 625 (1968). 32

Commonwealth v. Snow,
96 Mass. App. Ct. 672 (2019) 31

Commonwealth v. White,
475 Mass. 583 (2016) ..... *passim*

Glik v. Cunniffe,
655 F.3d 78 (1st Cir. 2011) 21

Riley v. California,
573 U.S. 373 (2014) ..... *passim*

Ybarra v. Illinois,
444 U.S. 851 (1979) 37

STATUTES, REGULATIONS AND RULES

18 U.S.C. 2102(b)..... 36

Mass. Gen. Laws ch. 269 § 1-2..... 36

OTHER AUTHORITIES

A. Smith, Pew Research Center, *Smartphone Ownership—2013 Update* (June 5, 2013) 18

Aaron Smith, *Americans' experiences with data security*, Pew Research Center (Jan. 26, 2017) 20

Andrew Perrin and Erica Turner, *Smartphones help blacks, Hispanics bridge some – but not all – digital gaps with whites*, Pew Research Center (Aug. 20, 2019) .. 22

Bill Chappell, *Fort Worth Police Drop Rioting Charges Against Protesters*, NPR (June 9, 2020). 36

BPD News, *BPD Confirms Fifty-Three Arrests Made and One Summons Issued Following Protests in Boston* (June 1, 2020). 35

Emily A. Vogels, *Millennials stand out for their technology use, but older generations also embrace digital life*, Pew Research Center (Sept. 9, 2019). 18

Monica Anderson & Emily A. Vogels, *Americans turn to technology during COVID-19 outbreak*, Pew Research Center (March 31, 2020). 22

Ryan Deto, *Pittsburgh's first two BLM protests led to dozens of arrests; about 90% of those charges have been dropped*, Pittsburgh City Paper (June 19, 2020). ... 36

Samantha Fields, *What it can cost to get arrested at a protest*, Marketplace (June 10, 2020). 35

Sarah Perez, *Report: Smartphone owners are using 9 apps per day, 30 per month*, TechCrunch (May 4, 2017) ... 19

Sujeong Lim, *Average Storage Capacity in Smartphones to Cross 80GB by End-2019*, Counterpoint (Mar. 16, 2019) 19

US Virtual Care Visits To Soar To More Than 1 Billion, Forrester (Apr. 10, 2020). 22

Whitney Woodworth, *Criminal charges dismissed against 14 arrested at Black Lives Matter protests*, Statesman Journal (June 29, 2020). 36

CONSTITUTIONAL PROVISIONS

Mass. Declarations of Rights, Art. 14..... *passim*

U.S. Const. amend. 4..... *passim*

CORPORATE DISCLOSURE STATEMENTS

Pursuant to Supreme Judicial Court Rule 1:21, the American Civil Liberties Union of Massachusetts, Inc. (ACLUM) and the Electronic Frontier Foundation (EFF) represent that they are 501(c)(3) organizations under the laws of the Commonwealth of Massachusetts. ACLUM and EFF do not issue any stock or have any parent corporation, and no publicly held corporation owns stock in ACLUM or EFF.

PREPARATION OF AMICI BRIEF

Pursuant to Mass. R. App. 17(c)(5), as amended, 426 Mass. 1602 (1998), amici and their counsel declare that:

(a) no party or a party's counsel authored this brief in whole or in part;

(b) no party or a party's counsel contributed money to fund preparing or submitting the brief;

(c) no person or entity other than the amici curiae contributed money that was intended to fund preparing or submitting a brief; and

(d) counsel has not represented any party in this case or in proceedings involving similar issues, or any party in a case or legal transaction at issue in the present appeal.

STATEMENT OF INTERESTS OF AMICI

The ACLU of Massachusetts, Inc., an affiliate of the national ACLU, is a statewide nonprofit membership organization dedicated to the principle of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. The rights they defend through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures. *See, e.g.*, *Commonwealth v. Evelyn*, SJC-12808 (2020) (amicus); Commonwealth *v. Almonor*, 482 Mass. 35 (2019) (amicus); *Commonwealth v. Augustine*, 467 Mass. 230 (2014) (direct representation); *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (direct representation).

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that works to ensure technology supports freedom, justice, and innovation for all the people of the world. For 30 years, EFF has represented technology users' interests in court cases and broader policy debates. EFF has served as amicus in numerous cases addressing Fourth Amendment protections in the digital age, including *Augustine*, 467 Mass. 230; *Carpenter*, 138 S. Ct. 2206; and *Riley v. California*, 573 U.S. 373 (2014).

INTRODUCTION

Less than four years ago, in *Commonwealth v. White*, the Court held that a police detective's opinion that a cell phone was likely to contain evidence did not establish probable cause to search the phone, absent a "substantial basis" for concluding that the phone contained evidence of the crime under investigation. 475 Mass. 583, 588-89 (2016). Even a "[s]trong reason to suspect is not adequate," the Court explained, nor is "probable cause to suspect the defendant of a crime." *Id.* at 589, 590. Rather, "police may not seize or search [a] cellular telephone to look for evidence unless they have information establishing the existence of particularized evidence likely to be found there." *Id.* at 590-91.

But there will always be *some* facts whenever the police arrest someone with a cell phone. And particularly when the arrestee has been charged with a serious offense, law enforcement will be tempted to say those facts, whatever they are, pass the *White* test and justify a warrant to search that phone. The inevitable attempts to distinguish *White* will, in turn, risk weakening this Court's holding in that case and, with it, the constitutionally protected privacy rights of people who use cell phones.

That risk is present here. Defendant Dondre Snow is accused of participating in a murder with Dwayne Diggs.

Snow was the driver of the vehicle in which Diggs was found after Diggs shot and killed the victim. Snow had a cell phone. At the time of his arrest, he used that phone to call his girlfriend who had a possessory interest in the car he was driving so that she could retrieve the car rather than have the police tow it. Snow's cell phone was seized by police incident to his arrest. The victim's cell phone was recovered at the scene of the shooting. On the victim's cell phone were threatening messages from Diggs; there were none from Snow. Based on this information, eighty days after Snow's phone was seized, the police obtained a warrant to search it. The motion judge suppressed the evidence from that search, but a divided panel of the Appeals Court reversed the suppression order.

The Commonwealth now argues that the search passed the *White* test, based on evidence showing little more than defendant's propinquity to another who has committed a crime and his possession of a cell phone. This argument, if accepted, could undermine *White*, weaken privacy interests of cell phone users protected by the Fourth Amendment to the U.S. Constitution and Article 14 of the Massachusetts Declarations of Rights, and take the Commonwealth closer to a rule that would permit the police to search the cell phone of virtually every person arrested for a crime.

It is fitting that the Commonwealth appears to hope that this case, *Snow*, will turn out differently than the last case, *White*. In the fairy tale *Snow White*, the Queen asks a question again and again to the "mirror, mirror on the wall," hoping for a desired answer. But in court, repeating the same question should yield the same answer. The Court struck the correct balance in *White*. It should maintain that balance here in *Snow* and decline the Commonwealth's invitation to rely on insubstantial facts to establish probable cause to search a phone.

STATEMENTS OF THE FACTS AND CASE[1]

On the night of December 5, 2015, a person was shot multiple times in South Boston. R. 56. The shooter, later identified as Dwayne Diggs, was seen getting into a car which sped away and ultimately parked on a dead-end street two miles away from the scene of the shooting. R. 56-57, 60. The car was later found to be driven by Dondre Snow. R. 58. A third person, Daquan Peters, was also in the car. *Id.*

Police were alerted to the presence of the vehicle by an emergency call. R. 57. Police responded to the call and arrested each of the car's occupants. R. 57-58. At the time of the arrest, Snow was talking on his cell phone to his girlfriend, who had rented the vehicle

[1] "(CA._)" herein refers to the Commonwealth's record appendix. "(R._)" herein refers to the defendant-appellee's record appendix.

he was driving, to inform her of the arrest. R. 58, 59. Snow and Diggs both wore Electronic Monitoring bracelets on their ankles. R. 61.

Snow was later indicted for murder, possessing a firearm without a license, possessing ammunition without an FID card, and carrying a loaded firearm without a license. CA. 3-8. When police arrested Snow, they did what is, today, commonplace: they seized his cell phone incident to arrest. But, uncommonly, police waited nearly 80 days before seeking a warrant to search the phone. R. 62, ¶ 23.

The warrant affidavit relied primarily on three facts to assert probable cause: (1) that Snow was talking on his phone shortly before his arrest, CA. 28, ¶ 8; (2) that an alleged co-venturer, Diggs, had previously sent threatening messages to the victim, CA. 32, ¶¶ 22-23; and (3) that, given the suspected coordination of the alleged offense, CA. 34, ¶ 30, evidence of the crime likely existed on the phone.

The affidavit states, "[T]here is probable cause to believe that a cellular phone that contains communications with others, in the time before and immediately after the incident . . . may lead to relevant evidence of intent, motive and may provide additional answers as to the facts and circumstances." R. 64. It further averred that "there is probable cause to believe that photographs and contacts contained within the

target phone may lead to the identity of other potential witnesses." *Id.* And it seeks permission to search a wide swath of data "[d]ue to the fact that it is unknown as to when the weapon was acquired and when any related conspiracy may have been formed." *Id.*

The warrant was granted, and it authorized police to search nearly every conceivable aspect of the phone, including:

> Cellular telephone number; electronic serial number, international mobile equipment identity, mobile equipment identifier or other similar identification number; address book; contact list; personal calendar, date book entries, and to-do lists; saved, opened, unopened, draft, sent, and deleted electronic mail; incoming, outgoing, draft, and deleted text messages and video messages; history of calls sent, received, and missed; any voicemail messages, including those that are opened, unopened, saved, or deleted; any photographs or videos, including those stored, saved, or deleted; any audio or video 'memos' stored, saved, or deleted; GPS information; mobile instant message chat logs, data and contact information; Internet browser history; and any and all of the fruits or instrumentalities of the crime of [m]urder.

CA. 23.

After his first trial ended in a mistrial, R. 46-47, the Commonwealth indicated, for the first time, that, in the second trial, it intended to introduce evidence obtained from the search of his cell phone. Snow filed a motion to suppress. R. 48.

The trial court allowed Snow's motion. R. 90. The court determined that the affidavit in support of the warrant to search Snow's cell phone failed to "establish the requisite nexus between" the murder and Snow's cell phone; "it does not establish the existence of some particularized evidence related to the crime likely to be found" on the cell phone; "and therefore, does not establish probable cause to search the defendant's cellular telephone." R. 90.

A divided Appeals Court reversed. R. 1-32. In doing so, the court relied on three factors: (1) an inference that the shooting, which was allegedly committed by two people wearing GPS tracking anklets, required planning and coordination, (2) Snow's cell phone was in the car, and he spoke with his girlfriend, whose car he drove, using that phone at the time of his arrest, and (3) Diggs exchanged violent text messages with the victim. R. 13-15.

Snow filed for further appellate review and, on April 17, 2020, this Court allowed the application. On April 22, this Court solicited the participation of amici. CA. 92.

SUMMARY OF ARGUMENT

Consistent with this Court's decision in *White*, probable cause to search a cell phone does not arise from: (1) a person's possession and unrelated use of a cell phone at the time of their arrest and (2) an assumption that because people often communicate through cell phones, alleged co-venturers likewise communicated through cell phones. For the following reasons, a contrary conclusion would foster precisely the problems that the Court sought to avoid when it decided *White*, namely unwarranted and frequent invasions of the most private aspects of a person's life.

I. As the Supreme Court, this Court, and other courts have repeatedly recognized, cell phones contain vast amounts of sensitive information about users. Cell phones are uniquely important especially now—both in light of the ongoing global pandemic and the role cell phones have played in documenting police violence and coordinating protests against that violence, and are deserving of stringent privacy protections. (pp 11-16).

II. Because cell phones contain vast amounts of sensitive data, the U.S. Supreme Court held in *Riley* that police must obtain a warrant based on probable cause before searching a cell phone. And this Court held in *White* that police must have a substantial basis to believe that particularized evidence related to the crime under investigation exists on the phone to be

searched. *White* further held that neither an officer's training and experience nor probable cause to believe that a person participated in a crime are sufficient to establish the requisite nexus. (pp 17-20).

III. This Court should reaffirm the *White* test and the considerations that caused the Court to adopt it. Endorsing the Commonwealth's approach, and allowing proximity to a crime combined with unrelated use of a cell phone to justify a finding of probable cause, could license invasions of privacy in many cases. (pp 21-31).

ARGUMENT

I. Cell phones are ubiquitous features of everyday life, with the capacity to store vast amounts of personal data.

This Court has repeatedly recognized that individuals have "significant privacy interests at stake in their cellular phones and that the probable cause requirement under both the Fourth Amendment and art. 14 must serve to protect these interests." *White*, 475 Mass. at 592 (quoting *Commonwealth v. Dorelas*, 473 Mass. 496, 502 n. 11 (2016)). Among myriad other uses, phones have become essential tools used for exercising First Amendment rights, documenting law enforcement abuses and governmental overreach, and communicating with doctors, teachers, and loved ones—*especially* during the ongoing COVID-19 pandemic.

A. Cell phones contain a vast amount of private data about their users.

Ninety-six percent of American adults own a cell phone, with 81 percent owning a smartphone.[2] For younger people that number is even higher; 93% of people between ages 23 to 38 now own smartphones.[3] "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Riley v. U.S.*, 573 U.S. 373, 395 (2014).

The Supreme Court recognized in *Riley* that cell phones are distinct from physical objects and containers in both quantitative and qualitative respects. Quantitatively, the sheer volume of information available on cell phones makes them fundamentally different from any pre-digital counterpart. With their "immense storage capacity," cell phones and other electronic devices can contain the equivalent of "millions of pages of text, thousands of pictures, or

---

[2] Pew Research Center, *Mobile Fact Sheet* (June 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/. *Cf. Riley*, 573 U.S. at 385 (citing A. Smith, Pew Research Center, *Smartphone Ownership—2013 Update* (June 5, 2013) (noting "56% of American adults are now smartphone owners")).

[3] Emily A. Vogels, *Millennials stand out for their technology use, but older generations also embrace digital life*, Pew Research Center (Sept. 9, 2019), https://pewresearch-org-preprod.go-vip.co/fact-tank/2019/09/09/us-generations-technology-use/.

hundreds of videos." *Id.* at 393, 394. The storage capacity of the average smartphone today—at over 80 gigabytes[4]—is five times as large as when *Riley* was decided just six years ago. *See id.* at 394 (16 gigabytes). The storage capacity of phones, and thus the quantity of personal information they contain, will only continue to increase.[5]

Qualitatively, cell phones "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record." *Riley*, 573 U.S. at 394. Average smartphone users now have 60-90 different apps on their devices and use 30 different apps per month.[6] Apps generate vast and varied data, including call logs, emails, text messages, voicemails, browsing history, calendar entries, contact lists, shopping lists, notes, photos and videos, books read, TV shows and movies watched, financial and health data, purchase history, dating profiles, metadata, and

---

[4] Sujeong Lim, *Average Storage Capacity in Smartphones to Cross 80GB by End-2019*, Counterpoint (Mar. 16, 2019), https://www.counterpointresearch.com/average-storage-capacity-smartphones-cross-80gb-end-2019.

[5] Lim, *supra* note 4.

[6] *See Riley*, 573 U.S. at 396 (describing various apps and noting, at that time, that the average smartphone user "has installed 33 apps, which together can form a revealing montage of the user's life."); Sarah Perez, *Report: Smartphone owners are using 9 apps per day, 30 per month*, TechCrunch (May 4, 2017), https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month.

so much more. This information, in turn, can reveal an individual's political affiliations, religious beliefs and practices, sexual and romantic life, financial status, health conditions, and family and professional associations. *See id.* at 394-96.

The ability of cell phones to access data that is not stored on the phone itself but in the "cloud," *i.e.*, on a server elsewhere, "further complicate[s] the scope of the privacy interest at stake." *Riley*, 573 U.S. at 397. "Virtually any digital action that internet users may take—from using credit cards to logging into social media sites—creates data that is stored by companies, governments or other organizations."[7] Although the information stored in the cloud should not be accessed by law enforcement who are searching through a phone, "officers searching a phone's data would not typically know whether the information they are viewing was stored locally . . . or has been pulled from the cloud." *Riley*, 573 U.S. at 397.

B. Cell phones are unique tools for exercising constitutional rights and conducting private communications.

Cell phones play an indispensable role in the modern world, especially in facilitating the exercise of

[7] Aaron Smith, *Americans' experiences with data security*, Pew Research Center (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security.

people's First Amendment rights to association and expression.

Today, it is the rare newsworthy event that is not captured on a cell phone video, notably including incidents of official misconduct and police brutality. *See, e.g.*, *Glik v. Cunniffe*, 655 F.3d 78, 79 (1st Cir. 2011) (First Amendment protected individual who used cell phone to record police conduct in public). And when these cell phone videos spur widespread protest—as with the unprecedented response to the video-recorded killing of George Floyd by Minneapolis police officers—individuals use their phones to coordinate marches, demonstrations, and collective action.

Phones are also central to the privacy of modern communications, particularly for those who use their phones as a primary or even sole means of connecting to the Internet. In 2019, 17% of Americans were "mobile dependent," meaning they owned a smartphone but did not have a home broadband connection.[8] The people in this group were more likely to be young, Black or Hispanic, and lower-income.[9] And Black and Hispanic people were accordingly found more likely than whites to rely on

[8] Pew Research Center, *Mobile Fact Sheet*, *supra* note 2.
[9] *Id.*

their smartphones for a number of activities such as seeking health information or looking for work.[10]

The ongoing COVID-19 pandemic has further increased the use of technology to communicate, as many conversations that might have otherwise been face-to-face are now conducted through FaceTime or Zoom. Children attend school, doctors treat patients,[11] and family, friends, and lovers meet—all online and frequently on a mobile device. Roughly 76% of Americans are estimated to be using email or messaging services to communicate with others during the pandemic, while 70% have searched online for health information about the coronavirus.[12]

As a result of the COVID-19 crisis, the data on our phones reveals even more, and even more private, information about our lives.

---

[10] Andrew Perrin and Erica Turner, *Smartphones help blacks, Hispanics bridge some – but not all – digital gaps with whites*, Pew Research Center (Aug. 20, 2019), https://www.pewresearch.org/fact-tank/2019/08/20/smartphones-help-blacks-hispanics-bridge-some-but-not-all-digital-gaps-with-whites/.

[11] *US Virtual Care Visits To Soar To More Than 1 Billion*, Forrester (Apr. 10, 2020) https://go.forrester.com/press-newsroom/us-virtual-care-visits-to-soar-to-more-than-1-billion/.

[12] Monica Anderson & Emily A. Vogels, *Americans turn to technology during COVID-19 outbreak*, Pew Research Center (March 31, 2020), https://www.pewresearch.org/fact-tank/2020/03/31/americans-turn-to-technology-during-covid-19-outbreak-say-an-outage-would-be-a-problem/.

II. This Court has determined that the vast storage and communications capacities of cell phones cannot automatically establish probable cause to search and seize a person's cell phone.

Decisions by the Supreme Court and this Court make clear that the vast quantities of private information stored on cell phones supply a reason to enforce, rather than ease, constitutional protections that stand between that information and law enforcement. In *Riley*, 573 U.S. at 394, the Supreme Court recognized that cell phones can reconstruct an individual's life, and the Court therefore held that the Fourth Amendment does not permit police to conduct a warrantless search of a cell phone incident to arrest. In *Dorelas*, this Court explained that, due to a cell phone's "distinct" qualities, a search of its many files must be done with special care" and "satisfy a more narrow and demanding standard." 473 Mass. at 502. And in *White*, this Court concluded that before a cell phone can be searched, Article 14 and the Fourth Amendment require probable cause that "some particularized evidence related to the crime" exists on the phone. 475 Mass. at 589 (internal quotations omitted). The decision in this case should follow that same approach.

A. The Supreme Court has limited searches of cell phones incident to arrest because they contain vast, private, and sensitive information.

Although it did not involve the precise legal issues presented here, the Supreme Court's decision in

Riley, concerning warrantless searches of cell phones incident to arrest, can inform this Court's decision-making about the quantum of evidence that police must demonstrate in order to obtain a warrant to search the phone of an arrestee. *Riley* turned, in significant part, on the fact that cell phones have become so central to daily life "that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." 573 U.S. at 385. Cell phones are "not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Id.* at 403. (quoting *Boyd v. U.S.*, 116 U.S. 616, 630 (1886)).

The Supreme Court's fundamental conclusion in Riley, that police must "get a warrant" to search the phone of an arrestee, would mean very little if the ability to obtain a warrant was an automatic consequence of making an arrest. That cell phones are capable of holding tremendous amounts of information is a reason to require a meaningful showing of probable cause; it is not a reason to say that probable cause has been established by the arrestee's use of the phone. *Cf. id.* at 386; *Commonwealth v. Augustine*, 472 Mass. 448, 455 (2015).

B. *White* requires probable cause to believe that particularized evidence related to the crime under investigation exists on the cell phone.

In *White*, a police detective seized the cell phone of a person suspected to have participated in an armed robbery and shooting. 475 Mass. at 586. At the time of the seizure, which preceded the defendant's arrest, police had information from the defendant's mother about defendant's involvement in the robbery and, from a consent search of the defendant's bedroom, had retrieved a jacket similar to one worn by one of the perpetrators. *Id.* at 585. What police did not have was "any information that a cell phone was used in the" robbery and shooting, "nor did they claim that there existed a particular piece of evidence likely to found on such a device." *Id.* at 590 (internal marks omitted). Instead, "they were aware, based on their experience, that such devices often contained useful information in cases involving multiple perpetrators." *Id.* at 586.

The Court held that police lacked probable cause to seize the phone. *Id.* at 592. In doing so, the Court established that police may not base probable cause determinations solely on: (1) the existence of evidence that multiple people participated in a crime; and (2) the belief, based on officers' training and experience, that "if the defendant planned and committed [the crime] with two coventurers, it was likely he did so, at least in part using his cellular telephone," and that,

therefore, his cell phone will likely contain communications with his co-venturers. *Id.* at 590, 591. "[S]uch considerations 'do not, alone, furnish the requisite nexus between the criminal activity and the places to be searched' or seized." *Id.* at 591 (quoting *Commonwealth v. Anthony*, 451 Mass. 59, 72 (2008)).

There must instead be "a substantial basis" for concluding that the cell phone contains "particularized evidence" connected or related to the crime under investigation. *Id.* at 588-89. This is so "even where there is probable cause to suspect the defendant of a crime. *Id.* at 590. "Only then . . . do [police] have probable cause to seize and search the device in pursuit of evidence." *Id.* at 589; *see also In re Search of Certain Cell Phones*, 541 F. Supp. 2d 1, 2 (D.D.C. 2008) (holding that, to establish probable cause, there must be some specific and objective "indication that the [cell phone] owner ever used the phone" in relation to the crime); *see also People v. Taylor*, 2002 WL 465094, at *16 (N.Y. Sup. Ct. Mar. 20, 2002) (holding a probable cause justification was merely "speculative" where police inferred from the defendant's use of his phone that he may have also used it "for other similar purposes" in relation to the crime).

III. This Court should reaffirm *White*'s holding that police need particularized evidence connecting the cell phone to be searched with the crime under investigation.

The Commonwealth's arguments, in effect, ask this Court to weaken its decision in *White*. The Court should not do so, lest it license significant invasions of privacy based on nothing more than someone's use of a phone while physically proximate to someone involved in a crime.

A. Mere presence and use of a cell phone at the scene of an arrest fails to establish probable cause to search the device.

Probable cause requires a nexus between the crime under investigation and the cell phone to be searched. *White*, 475 Mass. at 588. Precisely because cell phones are such an integral part of modern life, it will almost always be possible for the Commonwealth to hypothesize that an arrestee may have used his phone to commit the crime under investigation. But the Commonwealth's argument in this case fails to demonstrate the nexus that *White* requires, even when considering all reasonable inferences which may be drawn from the information in the warrant affidavit.

The Commonwealth argues that because (1) a passenger in Snow's car was suspected of having committed a crime and had previously communicated with the victim; (2) there were three people in the car "each of whom had a cell phone with him inside the vehicle";

and (3) Snow spoke with his girlfriend at the time of his arrest[13] in order to apprise her of the arrest itself, the police could infer that his cell phone would contain evidence linking him to the crime. *See* Com. Br. at 21, 24, 26, 31-32.

First, it is unclear how communications between *Diggs* and the victim, combined with the presence of Diggs in Snow's car after the murder, establish a nexus between *Snow's* phone and the crime. Probable cause to search someone's cell phone seems unlikely to arise from how an acquaintance of that person has chosen to use their cell phone. *Cf. Commonwealth v. Morin*, 478 Mass. 415, 426 (2017) ("information that an individual communicated with another person, who may have been linked to a crime, without more, is insufficient to establish probable cause to search either individual's cellular telephone"); *Buckham v. State*, 185 A.3d 1, 17 (Del. 2018) ("Particularly unpersuasive was the statement that 'criminals often communicate through cellular phones' (who doesn't in this day and age?) and the statement that Waters' girlfriend—who owns the vehicle that Waters was allegedly driving on the day of the shooting—'contacted Buckham's girlfriend via cell phone' before she spoke with the police about the incident, which

[13] *Amici* read the record as suggesting only that Snow was talking on his cell phone when it became clear that he was about to be arrested. Com. Br. at 11, 13.

provides no basis at all to suspect that Buckham's cell phone was likely to contain evidence.").

Second, probable cause to search a phone cannot be said to arise from the fact that the crime under investigation may have involved multiple perpetrators. *Morin*, 478 Mass. at 426 ("police may not rely on the general ubiquitous presence of cellular telephones in daily life, or an inference that friends or associates most often communicate by cellular telephone, as a substitute for particularized information that a specific device contains evidence of a crime"). As applied here, the fact that Snow, Diggs, and Peters were in a car and, like 96% of American adults, they each had a cell phone would not establish probable cause to believe that they communicated using their cell phones to plan a murder. *See Commonwealth v. Jordan*, 91 Mass. App. Ct. 743, 750 (2017) (to establish probable cause to retrieve data from a cell phone, it is not enough to rely on "generalities that friends or coventurers often use cellular telephones to communicate"). Importantly, the Commonwealth has presented no evidence to suggest, and nothing in the record supports a finding, that this murder was either planned or coordinated, let alone planned or coordinated through cell phone communications. *See* Com. Br. At 40-43; compare *Commonwealth v. Holley,* 478 Mass. 508, 526 (2017) (defendants, who lived separately, arrived at victim's

house at the same time and were both seen on their cell phones); *Commonwealth v. Arthur*, 94 Mass. App. Ct. 161, 165 (2018) (co-venturers arrived together in two separate cars and left their vehicles in sequence while leaving the engine running).

Instead, the Commonwealth attempts to argue that probable cause exists because the police believed that *if* these three individuals *had* planned and committed the murder, it was likely they had communicated by using their cell phones, and accordingly, likely that evidence of these communications would be found on the device. Com. Br. at 31-32; *see also* R. 64 (warrant affidavit).

This same argument was rejected by the Court in *White*. 475 Mass. at 590. As the Court explained there, the mere possibility that a person could keep on their cell phone a digital record of communications with their co-venturers, without more, is not enough to establish probable cause. *Id.* at 591; *see also Commonwealth v. Broom*, 474 Mass. 486, 496-497 (2016) (“general” and “conclusory” opinion by affiant that individual is likely to store information in cell phone does not satisfy probable cause standard).

Third, an arrestee’s use of a cell phone at the time of arrest, especially without proof that he used the phone at any time during the commission of the alleged crime, cannot satisfy probable cause. Therefore, that Snow called his girlfriend to apprise her of his

arrest so that she may retrieve her car does not establish probable cause.[14] *See Buckham*, 185 A.3d at 17 ("the fact that [defendant] may have been using his phone to talk about his impending arrest connects his phone to the arrest warrant, not the underlying crime."); *see also Jordan*, 91 Mass. App. Ct. at 750-51 (declining to find probable cause based on evidence that defendant called two family members around the time of the murder). As Judge Henry wrote in dissenting from the Appeals Court's decision, the logic of the Commonwealth's argument is that "although the ubiquity of cell phones cannot justify a search, if a person actually uses rather than just carries that cell phone shortly after committing a crime, then the cell phone is probably connected to the crime and subject to search." *Commonwealth v. Snow*, 96 Mass. App. Ct. 672, 681 (2019) (Henry, J. dissenting in part, concurring in part). The Commonwealth's logic would justify a finding of probable cause anytime it can be shown that a person suspected of a crime used their cell phone, for any reason, in close

[14] Although the Commonwealth argues that Snow "was trying to ensure that the car used in the shooting did not remain in police custody," Com. Br. at 23, the warrant affidavit clearly states that the police had already conducted a search of the vehicle (with the consent of Snow's girlfriend) and found no evidence to support an inference that the vehicle would need to be hidden in order to destroy evidence. R. 59.

temporal proximity to the commission of a crime.[15] This will presumably be an easy showing given that, for many people, cell phone use is constant.

In short, "the affidavit made no connection between the defendant's use of his cellular telephone and his involvement in the crime." *See Jordan*, 91 Mass. App. Ct. at 751. This is insufficient to establish probable cause under *White*.

B. The Commonwealth's inability to identify a timeframe or location for any alleged evidence on the phone further underscores their lack of probable cause.

The absence of probable cause to search Snow's cell phone is also reflected in the boundless scope of the requested search. Search warrants must clearly define and limit the scope of the search. *Commonwealth v. Pope*, 354 Mass. 625, 629 (1968). The particularity requirement protects individuals from the general searches allowed under the "reviled 'general warrants' and 'writs of

[15] In fact, this Court recently held in *Commonwealth v. Goncalves-Mendez*, that it is "the better practice" for police to inform an individual, prior to seizing his car upon arrest, "that the vehicle will be taken to a police facility or private storage facility for safekeeping unless the driver directs the officer to dispose of it in some lawful manner." 484 Mass. 80, 85 n.8 (2020). Snow telephoned his girlfriend, who had lawful possessory interest in the car, so that she may retain custody of the vehicle rather than have the police tow it. Yet, here, Snow's exercise of his art. 14 rights is being proffered as evidence of criminality. Com. Br. at 23.

assistance' of the colonial era." *Riley*, 373 U.S. at 403.

Despite this requirement, the Boston Police Department submitted a warrant application on February 23, 2016, more than 80 days after having seized Snow's cell phone, to search virtually all data on the phone "without date restriction." R. 52, 64. This unfettered search was requested, it seems, not because the BPD had evidence of the requisite nexus between the crime alleged and the cell phone to be searched, *see* R. 64-65, but precisely because the BPD lacked such evidence. The warrant application could not say where incriminating evidence could be expected to be found on the cell phone because law enforcement lacked evidence to suggest there was a conspiracy between Snow and Diggs; when such conspiracy formed (if it existed at all); and when the murder weapon was acquired (and presumably who acquired it). R. 64.

Thus, the BPD was constrained to request authorization to comb through information stored on Snow's phone, "including but not limited to" the 13 data storage locations specified in the affidavit and application as well as "any and all of the fruits or instrumentalities of the crime of Murder." R. 65. But such grasping for evidence runs directly counter to the particularity requirement, which "serves as a safeguard against general exploratory rummaging by police through

a person's belongings." *Commonwealth v. Freiberg*, 405 Mass. 282, 298 (1989). The Commonwealth's inability to specify what exactly it was searching for was a reason for the warrant application to be rejected, rather than for it to proceed without any meaningful constraint on its scope.

C. The Commonwealth's approach threatens privacy.

Accepting the Commonwealth's arguments in this case would risk creating the very situation that this Court sought to avoid in *White*, namely that "it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search." *White*, 475 Mass. at 591. Under the Commonwealth's approach, police could have license to search the phone of anyone who merely happens to be nearby when a crime involving more than one person is alleged to have occurred. This would have a disproportionate impact on the privacy interests of law-abiding people engaged in peaceful protest throughout the Commonwealth.

For example, the country has been experiencing nationwide protests against police brutality in the wake of George Floyd's death at the knee of a police officer. Not only was his death-and the death of many other Black Americans-captured on cell phone, which galvanized people to take to the streets to push for police reform, but the activities of police in response to those initial

protests were captured on cell phone as well. These cell phone videos opened the eyes of even more Americans and people around the world to the indignities police perpetrate on communities of color every day. None of these events could have been recorded if not for the fact that these protestors took their phones to and used them at the protests.

However, by early June, in response to these protests, police across the country had arrested over 10,000 people, many for low-level offenses such as curfew violation or failure to disperse.[16] In Boston, 11 people were arrested solely on charges of disorderly conduct and/or disturbing the peace following the protest on May 31.[17] As a matter of routine during mass arrests, police seized cell phones and other personal possessions incident to arrest,[18] even though many cities

---

[16] Anita Snow, *AP tally: Arrests at widespread US protests hit 10,000*, AP (June 4, 2020), https://apnews.com/bb2404f9b13c8b53b94c73f818f6a0b7.

[17] BPD News, *BPD Confirms Fifty-Three Arrests Made and One Summons Issued Following Protests in Boston* (June 1, 2020), https://bpdnews.com/news/2020/6/1/bpd-confirms-fifty-three-arrests-made-and-one-summons-issued-following-protests-in-boston.

[18] Samantha Fields, *What it can cost to get arrested at a protest*, Marketplace (June 10, 2020), https://www.marketplace.org/2020/06/10/what-it-can-cost-to-get-arrested-at-a-protest/.

quickly dropped or reduced charges against many of the arrestees.[19]

But if the Commonwealth's arguments prevail, arrests like these during political protests could potentially furnish police with everything they need to search seized phones. Many people bring phones to document protests; they may well be in the process of using a phone during an arrest (perhaps even to document the arrest itself); and they are standing amongst many other individuals engaged in similar protest activities. For example, during protests police frequently invoke crimes such as incitement to riot, which under both Massachusetts and federal law involve the participation of several people. *See, e.g.,* Mass. Gen. Laws ch. 269 §§ 1-2; 18 U.S.C. § 2102(b). Such a charge—even if dropped days later—could suggest "evidence of

[19] Bill Chappell, *Fort Worth Police Drop Rioting Charges Against Protesters*, NPR (June 9, 2020), https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/09/872827789/fort-worth-police-drop-rioting-charges-against-protesters-topic-of-a-broad-debat; Whitney Woodworth, *Criminal charges dismissed against 14 arrested at Black Lives Matter protests*, Statesman Journal (June 29, 2020), https://www.statesmanjournal.com/story/news/crime/2020/06/29/charges-dropped-black-lives-matter-salem-oregon-protests/3283065001/; Ryan Deto, *Pittsburgh's first two BLM protests led to dozens of arrests; about 90% of those charges have been dropped*, Pittsburgh City Paper (June 19, 2020), https://www.pghcitypaper.com/pittsburgh/pittsburghs-first-two-blm-protests-led-to-dozens-of-arrests-about-90-of-those-charges-have-been-dropped/Content?oid=17489183.

coordination" sufficient under the Commonwealth's reasoning to provide probable cause to search a seized phone.

The Fourth Amendment prohibits searches of individuals based on a "mere propinquity to others independently suspected of criminal activity." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). The need for independent probable cause to search a person is grounded in the important interest in "safeguarding citizens from rash and unreasonable interferences with privacy." *Id.* at 95-96 (citations omitted). Searches of cell phones should be no different, but the Commonwealth seeks to undermine that bedrock rule here.

Whether a person is arrested at a large protest or suspected of coordinating illegal acts with other occupants of a car, the mere propinquity of a cell phone to that activity does not constitute probable cause to search that device.

CONCLUSION

Amici respectfully ask the Court to affirm the *White* test and require a strict adherence to the requirement that, in seeking to establish probable cause to search a cell phone, the Commonwealth must establish a substantial basis for asserting that the phone contains evidence of a crime.

Respectfully submitted,

*/s/ Mark Rumold*_____ ___
Jennifer Lynch (CA 240701)
Andrew Crocker (CA 291596)
Mark Rumold (CA 279060)
Hannah Zhao (NY 5468673)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org

/s/ Jessica J. Lewis
Matthew R. Segal, BBO #654489
Jessie J. Rossman (BBO 670685)
Jessica J. Lewis, BBO #704229
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MASSACHUSETTS, INC.
211 Congress Street
Boston, MA 02110
(617) 482-3170
jlewis@aclum.org

Counsel for *Amici Curiae*

CERTIFICATE OF COMPLIANCE

I, Jessica Lewis, hereby certify that this brief complies with the rules of court pertaining to the filing of briefs, including, but not limited to: Mass. R. App. P. 16(a)(6) (pertinent findings or memorandum of decision); Mass. R. App. P. 16(e) (references to the record); Mass. R. App. P. 16(f) (reproduction of statutes, rules, regulations); Mass. R. App. P. 16(h) (length of briefs); Mass. R. App. P. 18 (appendix to the briefs); and Mass. R. App. P. 20 (form of briefs, appendices, and other papers).

/s/ Jessica J. Lewis
Jessica J. Lewis

AFFIDAVIT OF SERVICE

I, Jessica J. Lewis, counsel for the American Civil Liberties Union of Massachusetts, Inc. do hereby certify under the penalties of perjury that on this 28th day of August, 2020, I caused a true copy of the foregoing document to be served by electronic filing through the CM/ECF system on the following counsel and that paper copies will be sent to any non-registered participants:

Cailin M. Campbell
Chief of Appeals
Assistant District Attorney for the Suffolk District
One Bulfinch Pl.
Boston, MA 02114
cailin.campbell@state.ma.us
Counsel for the Commonwealth

Amy M. Belger
Law Office of Amy M. Belger
841 Washington Street
Holliston, MA 01746
appellatedefender@gmail.com
Counsel for Defendant-Appellee Dondre Snow

/s/ Jessica J. Lewis
Jessica J. Lewis

No. SJC-12938

Commonwealth of Massachusetts
Appellant

v.

Dondre Snow,
Defendant-Appellee.

ON APPEAL FROM A JUDGMENT OF
THE SUFFOLK SUPERIOR COURT

BRIEF AMICI CURIAE OF THE AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC. AND THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF THE APPELLEE
