

COMMONWEALTH OF MASSACHUSETTS  
SUPREME JUDICIAL COURT

---

No. SJC-11917

---

COMMONWEALTH OF MASSACHUSETTS  
Appellant

v.

ONYX WHITE  
Defendant-Appellee

---

ON APPEAL FROM A JUDGMENT OF  
THE SUFFOLK SUPERIOR COURT

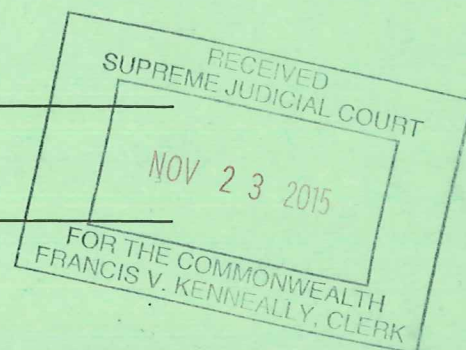
---

BRIEF FOR *AMICUS CURIAE*  
AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS  
IN SUPPORT OF THE DEFENDANT-APPELLEE

---

CYBERLAW CLINIC  
HARVARD LAW SCHOOL  
BERKMAN CENTER FOR INTERNET & SOCIETY

Vivek Krishnamurthy (BBO Number Pending)  
Andrew J. Sellars (BBO #682690)  
1585 Mass Ave., Suite 5018  
Cambridge, MA 02138  
Tel: (617) 495-7547  
Fax: (617) 495-7641  
vkrishnamurthy@cyber.law.harvard.edu  
asellars@cyber.law.harvard.edu



COMMONWEALTH OF MASSACHUSETTS  
SUPREME JUDICIAL COURT

---

No. SJC-11917

---

COMMONWEALTH OF MASSACHUSETTS  
Appellant  
v.  
ONYX WHITE  
Defendant-Appellee

---

ON APPEAL FROM A JUDGMENT OF  
THE SUFFOLK SUPERIOR COURT

---

BRIEF FOR *AMICUS CURIAE*  
AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS  
IN SUPPORT OF THE DEFENDANT-APPELLEE

---

CYBERLAW CLINIC  
HARVARD LAW SCHOOL  
BERKMAN CENTER FOR INTERNET & SOCIETY

Vivek Krishnamurthy (BBO Number Pending)  
Andrew J. Sellars (BBO #682690)  
1585 Mass Ave., Suite 5018  
Cambridge, MA 02138  
Tel: (617) 495-7547  
Fax: (617) 495-7641  
vkrishnamurthy@cyber.law.harvard.edu  
asellars@cyber.law.harvard.edu

On the brief:

Matthew R. Segal (BBO #654489)  
Jessie J. Rossman (BBO #670685)  
msegal@aclum.org  
jrossman@aclum.org  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF MASSACHUSETTS  
211 Congress Street  
Boston, MA 02110  
Tel: (617) 482-3170  
Fax: (617) 451-0009

## INTEREST OF THE *AMICUS CURIAE*

The American Civil Liberties Union of Massachusetts (“ACLUM”), an affiliate of the national American Civil Liberties Union, is a statewide membership organization dedicated to the principles of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. Among the rights that ACLUM defends through direct representation and amicus briefs is the right to be free from unreasonable searches and seizures. *See, e.g., Commonwealth v. Estabrook*, 472 Mass. 852, 38 N.E.3d 231, 234 (2015); *Commonwealth v. Augustine*, 467 Mass. 230 (2014). Accordingly, ACLUM has an interest in this case because it could significantly impact constitutional protections against unreasonable government access to cell phone data.

## TABLE OF CONTENTS

Introduction.....	8
Argument.....	10
1. Probable Cause to Seize and Search a Criminal Suspect's Cell Phone Is Not Automatically Established by the Vast Storage and Communications Capacities of Such Devices.....	10
1.1. The Vast Storage Capacity and Functionality of Cell Phones Does Not Automatically Establish Probable Cause. ....	13
1.2. The Fact That Cell Phones Allow People to Communicate and Thus Could be Used Commit Crimes Does Not Automatically Establish Probable Cause. ....	14
1.3. The Court Should Not Hollow the Probable Cause Requirement Here and License Invasions of Privacy. .....	16
2. Even When Probable Cause Exists, the Mere Possibility of Remote Wiping Does Not Automatically Establish an Exigent Circumstance.....	17
2.1. Remote Wipe Technology Does Not Automatically Establish an Exigent Circumstance. ....	18
2.2. Remote Wipe Technology Did Not Establish an Exigent Circumstance in This Case. ....	20
3. If a Cell Phone Is Seized, the Fourth Amendment Requires That A Warrant to Search It Must Be Obtained Without Undue Delay.....	22
3.1. Tolerance for Delay When Applying to Search a Computing Device Is Especially Low. ....	23
3.2. Without A Defendant's Consent To A Seizure, Long Delays In Obtaining A Warrant Are Not Reasonable. ....	25
3.3. A 68-Day Delay Between Seizing a Cell Phone and Seeking a Warrant Constitutes Undue Delay. ...	26
Conclusion.....	27

## TABLE OF AUTHORITIES

### MASSACHUSETTS CASES

<i>Commonwealth v. Anthony</i> , 451 Mass. 59 (2008).....	12
<i>Commonwealth v. Augustine</i> , 472 Mass. 448, 35 N.E.3d 688 (2015).....	13
<i>Commonwealth v. Cinelli</i> , 389 Mass. 197 (1983).....	11
<i>Commonwealth v. Cruz</i> , 430 Mass. 838 (2000).....	11, 12
<i>Commonwealth v. Damian D.</i> , 434 Mass. 725 (2001).....	11
<i>Commonwealth v. Diaz</i> , No. ESCR 2009-00060, 2009 WL 2963693 (Mass. Super. Sept. 3, 2009).....	15
<i>Commonwealth v. Estabrook</i> , 472 Mass. 852 (2015).....	9
<i>Commonwealth v. Kaupp</i> , 453 Mass. 102 (2009).....	24
<i>Commonwealth v. Pina</i> , 453 Mass. 438 (2009).....	12, 13
<i>Commonwealth v. White</i> , Mass. Super. Ct., No. 10-10511, slip. op. (May 23, 2014).....	16, 26

### FEDERAL CASES

<i>Anderson v. Creighton</i> , 483 U.S. 635 (1987).....	11
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	17
<i>In re Search of Certain Cell Phones</i> , 541 F. Supp. 2d 1 (D.D.C. 2008).....	15
<i>Kentucky v. King</i> , 563 U.S. 452 (2011).....	17, 19
<i>Michigan v. Tyler</i> , 436 U.S. 499 (1978).....	18
<i>Missouri v. McNeely</i> , 133 S. Ct. 1552 (2013).....	18
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	passim

<i>Schlossberg v. Solesbee</i> , 844 F. Supp. 2d 1165 (D. Or. 2012).....	21
<i>Segura v. U.S.</i> , 468 U.S. 796 (1984).....	22
<i>U.S. v. Aispuro</i> , No. 13-10036-01 MLB, 2013 WL 3820017 (D. Kan. July 24, 2013).....	19
<i>U.S. v. Burgard</i> , 675 F.3d 1029 (7th Cir. 2012)..	passim
<i>U.S. v. Camou</i> , 773 F.3d 932 (9th Cir. 2014).....	19
<i>U.S. v. Dass</i> , 849 F.2d 414 (9th Cir. 1988).....	22
<i>U.S. v. Gomez</i> , 807 F. Supp. 2d 1134 (S.D. Fla. 2011)	20
<i>U.S. v. Hayes</i> , 518 F.2d 675 (6th Cir. 1975).....	21
<i>U.S. v. Henry</i> , No. 2:14-CR-64-JDL, 2014 WL 5323613 (D. Me. Oct. 17, 2014).....	12
<i>U.S. v. Jarman</i> , 61 F. Supp. 3d 598 (M.D. La. 2014)..	25
<i>U.S. v. Jenkins</i> , No. 3:13-CR-30125-DRH-11, 2014 WL 2933192 (S.D. Ill. June 30, 2014).....	19
<i>U.S. v. Laist</i> , 702 F.3d at 613-14 (11th Cir. 2012).	23, 25
<i>U.S. v. Mitchell</i> , 565 F.3d 1347 (11th Cir. 2009)	22, 24, 26
<i>U.S. v. Place</i> , 462 U.S. 696 (1983).....	17, 23
<i>U.S. v. Respress</i> , 9 F.3d 483 (6th Cir. 1993)	11, 16, 22, 24
<i>U.S. v. Schultz</i> , 14 F.3d 1093 (6th Cir. 1994).....	14
<i>U.S. v. Scott</i> , 83 F. Supp. 2d 187 (D. Mass. 2000)...	12
<i>U.S. v. Stabile</i> , 633 F.3d 219 (3rd Cir. 2011).....	25
<i>U.S. v. Wurie</i> , 728 F.3d 1 (1st Cir. 2013).....	20
<i>U.S. v. Zaavedra</i> , No. 12-CR-156-GKF, 2013 WL 6438981 (N.D. Okla. Dec. 9, 2013).....	20

## **STATE CASES**

<i>People v. Shinohara</i> , 375 Ill. App. 3d 85 (2007).....	25
<i>People v. Taylor</i> , No. 1012/2001, 2002 WL 465094 (N.Y. Supp. Ct. Mar. 20, 2002).....	15
<i>State v. Hall</i> , 555 So. 2d 495 (La. Ct. App. 1989)...	19

## **MASSACHUSETTS CONSTITUTIONAL PROVISIONS**

Mass. Const. Pt. 1, art. XIV.....	11
-----------------------------------	----

## **FEDERAL CONSTITUTIONAL PROVISIONS**

U.S. Const. amend. IV.....	11
----------------------------	----



## INTRODUCTION

The Commonwealth's position in this appeal would permit it to seize virtually every criminal suspect's cellular phone—the most private item she owns—and hold it indefinitely without a warrant until it ultimately explores the cell phone's immense contents. Such sweeping views of probable cause, exigency, and delay turn the Fourth Amendment and Article 14 on their heads, and cannot be reconciled with legal precedent or sound policy.

The ubiquity of cellular telephones (“cell phones”), their powerful functionality, and their capacity to store enormous amounts of private information do not justify the Commonwealth's diluted version of individual privacy rights. To the contrary, these features are the reason courts have determined that cell phones require the most stringent constitutional protections—namely, a promptly obtained warrant supported by probable cause—whenever the government seeks to search or seize them. It would be passing strange, to say the least, for the very elements that trigger the need for a warrant to search or seize a cell phone to also automatically satisfy its probable cause requirement.

As this Court and the United States Supreme Court have recognized, individuals have a profound privacy

interest in their cell phones. *See Riley v. California*, 134 S. Ct. 2473, 2495 (2014); *Commonwealth v. Estabrook*, 472 Mass. 852 (2015); *Commonwealth v. Augustine*, 467 Mass. 230, 245 (2014). Cell phones harbor a microcosm of our lived experience and are an “indispensable part of modern [American] life.” *Id.* (internal quotation marks omitted); *see also Riley*, 134 S. Ct. at 2495. “The term ‘cell phone’ is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.” *Id.* at 2489. In carrying cell phones in their pockets, most citizens of the Commonwealth carry vast, private collections of their personal effects, communications, thoughts, and relationships with them wherever they go. *Id.* at 2490.

With all they contain and all they may reveal, cell phones hold for many Americans “the privacies of life.” *Id.* at 2495 (internal quotation marks omitted). This makes strict adherence to our cherished constitutional protections in searching and seizing such devices all the more important. Probable cause must always be found to search a cell phone; the fact that cell phones contain so much private information does not automatically

establish it. Exigent circumstances or another recognized warrant exception must be established to seize a cell phone without prior judicial authorization; the fact that cell phone data can be remotely erased does not automatically provide them. And undue delay in obtaining a warrant will render a seizure of a cell phone unlawful; indeed, the significance of these devices demands that they not be retained indefinitely by the police.

Accordingly, the court below properly found that the Commonwealth disregarded these firmly established constitutional protections in seizing a cell phone without a warrant, without probable cause, and without seeking a warrant for nearly ten weeks thereafter. The court below correctly assessed the Commonwealth's position for what it plainly is: a straightforward infringement of constitutional rights. Neither the Massachusetts Declaration of Rights nor the federal Bill of Rights can so easily yield in the face of new technology.

## **ARGUMENT**

### **1. PROBABLE CAUSE TO SEIZE AND SEARCH A CRIMINAL SUSPECT'S CELL PHONE IS NOT AUTOMATICALLY ESTABLISHED BY THE VAST STORAGE AND COMMUNICATIONS CAPACITIES OF SUCH DEVICES.**

Before a cell phone can be seized or searched, Article 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution re-

quire the establishment of probable cause. Mass. Const. Pt. 1, art. XIV; U.S. Const. amend. IV. Regardless of whether the search or seizure takes place pursuant to a warrant or one of the limited warrant requirement exceptions, probable cause is always required. *Id.*; *Anderson v. Creighton*, 483 U.S. 635, 657 (1987) (noting that courts reach question of exigency only once probable cause has been established). Critically, police must have probable cause at the moment of seizure to believe that the item contains evidence of a crime.<sup>1</sup> See *U.S. v. Respress*, 9 F.3d 483, 486-87 (6th Cir. 1993).

This Court has held that probable cause to search “demands more than mere suspicion” that incriminating evidence will be found. *Commonwealth v. Cruz*, 430 Mass. 838, 840 (2000). Moreover, probable cause to believe that “a person is guilty of a crime does not necessarily constitute probable cause to search.” *Commonwealth v. Cinelli*, 389 Mass. 197, 213, *cert. denied*, 464 U.S. 860 (1983). Rather, the government has the burden of

---

<sup>1</sup> Even though the seizure in this case occurred at a school, it was done by a police officer pursuant to an ongoing investigation into a crime that was committed entirely off school premises. Thus, the seizure does not fall into the lower constitutional standards applicable to school officials’ investigations of on-campus violations. See *Commonwealth v. Damian D.*, 434 Mass. 725, 728, 752 N.E.2d 679, 681 (2001). The Commonwealth does not argue for a lower standard on appeal.

showing “particularized information” sufficient to establish a nexus between the place to be searched and the crime. *Commonwealth v. Pina*, 453 Mass. 438, 439 (2009). There must be reason to believe that the specific items to be searched are “related to the criminal activity under investigation.” *Cruz*, 430 Mass. at 840.

In the digital context, law enforcement must provide reason to believe that the suspect’s device actually contains evidence of a particular crime. *See, e.g., Commonwealth v. Anthony*, 451 Mass. 59, 71 (2008) (finding probable cause to search defendant’s computers when he admitted to the police to viewing online child pornography); *U.S. v. Scott*, 83 F. Supp. 2d 187, 195-96 (D. Mass. 2000) (finding probable cause to search a computer where there was witness testimony and physical evidence that the defendant had produced forged checks from that computer); *U.S. v. Henry*, No. 2:14-CR-64-JDL, 2014 WL 5323613, at \*5, 14 (D. Me. Oct. 17, 2014) (finding probable cause to search a cell phone where there was witness testimony that the phone had been used to take photographs for the purposes of prostitution).

1.1. THE VAST STORAGE CAPACITY AND FUNCTIONALITY OF CELL PHONES DOES NOT AUTOMATICALLY ESTABLISH PROBABLE CAUSE.

The fact that cell phones are capable of holding tremendous amounts of information and performing a variety of tasks does not *ipso facto* establish probable cause to search them. These capabilities are the reason for requiring, not the basis of establishing, probable cause. *Cf. Riley*, 134 S. Ct. at 2483; *Commonwealth v. Augustine*, 472 Mass. 448, 35 N.E.3d 688, 694 (2015). The Court's deliberate protection of such private information would be rendered meaningless if its very existence always established probable cause.

Given the enormity of what can be stored on a cell phone, “[i]t would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone.” *Riley*, 134 S. Ct. at 2492. The Commonwealth argues that it would be “reasonable to believe” that the defendant would have been “communicating about the string of robberies [. . .] whether it be communications that reveal a plan, encouragement, or concealment” using his cell phone. Br. Appellant at 22. But such mere suppositions about a criminal suspect's cell phone – no matter how reasonable – do not give rise to probable cause or justify the cell phone's search and seizure. *Cf. Pina*, 453 Mass. at 440-41 (probable cause to search a house not

established by the fact that a drug dealer lived there); *see also U.S. v. Schultz*, 14 F.3d 1093, 1097-98 (6th Cir. 1994) (a “guess” that evidence will be found in a container is not enough).

1.2. THE FACT THAT CELL PHONES ALLOW PEOPLE TO COMMUNICATE AND THUS COULD BE USED COMMIT CRIMES DOES NOT AUTOMATICALLY ESTABLISH PROBABLE CAUSE.

The Commonwealth also argues that, because the defendant was suspected of having committed a crime “with at least one person and perhaps two people,” the police could infer that his cell phone would contain evidence linking him to those other people, since “cell phones contain contact lists and communications.” Br. Appellant at 19, 21. In other words, the Commonwealth alleges that probable cause was established because individuals can use their cell phones to communicate with other people to commit crimes.

Even if this inference was informed by a police officer’s training and experience, it too does *not* establish probable cause. *Cf. Schultz*, 14 F.3d 1097-98 (officer’s knowledge that safe deposit boxes commonly store records of drug distribution was not enough to establish probable cause). To hold otherwise would create the twenty-first century equivalent of “the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage

through homes in an unrestrained search for evidence of criminal activity.” *Riley*, 134 S. Ct. at 2494.

Rather, there must be some specific and objective “indication that the owner ever used the phone in any way [in relation to the crime].” *In re Search of Certain Cell Phones*, 541 F. Supp. 2d 1, 2 (D.D.C. 2008); *see also People v. Taylor*, No. 1012/2001, 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). For example, in *Commonwealth v. Diaz*, the court held that police did not have probable cause to search the cell phone of a suspected drug trafficker, because they “never observed [the defendant] communicate on his cellular telephone,” and had “no principled way of distinguishing” between communications on that phone “that were likely to be perfectly lawful, and those calls that might produce evidence of criminality.” No. ESCR 2009-00060, 2009 WL 2963693, at \*8 (Mass. Super. Sept. 3, 2009).

Here, the police had no contemporaneous information that the defendant’s cell phone contained evidence of a crime.<sup>2</sup> The Commonwealth did no more than suggest that

---

<sup>2</sup> The search warrant application in this case relies upon an April 21, 2010 interview, which mentions a pos-



a cell phone owner committed a crime with several others. Such an assertion simply does not establish probable cause to search an individual's most private possession.

1.3. THE COURT SHOULD NOT HOLLOW THE PROBABLE CAUSE REQUIREMENT HERE AND LICENSE INVASIONS OF PRIVACY.

It cannot be that probable cause automatically exists to search the cell phone of anyone suspected of committing a crime with others, by virtue of the cell phone's capability to store information and communicate with others. This would eviscerate the protections of the Fourth Amendment and Article Fourteen in our new technological age. Probable cause requires more than owning a working cell phone.

Finding probable cause here would have serious consequences. Cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 134 S. Ct. at 2484.

---

sible photograph on the defendant's phone. *Commonwealth v. White*, Mass. Super. Ct., No. 10-10511, slip op. (May 29, 2014) at 2. Because this interview took place two months after the phone had been seized, *id.*, it cannot be used to establish probable cause to support the seizure, *cf. Respress*, 9. F.3d at 486. The Commonwealth does not dispute this in its brief. Without the photograph, however, only speculation about the evidentiary value of the cell phone remained, and the warrant application should therefore have been denied.

Cell phones are ubiquitous and contain all the “the privacies of life.” *Id.* at 2495 (internal quotation marks omitted). Thus, to find probable cause here would be to grant law enforcement a general warrant to invade virtually every criminal suspect’s private storehouse of their thoughts, feelings, conversations, and relationships. This result is anathema to Article Fourteen and the Fourth Amendment.

**2. EVEN WHEN PROBABLE CAUSE EXISTS, THE MERE POSSIBILITY OF REMOTE WIPING DOES NOT AUTOMATICALLY ESTABLISH AN EXIGENT CIRCUMSTANCE.**

Even when probable cause exists, warrantless seizures are presumed unreasonable. *U.S. v. Place*, 462 U.S. 696, 701 (1983). The government bears the burden to establish that any such seizures fit within the few “jealously and carefully drawn” exceptions to the warrant requirement. *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971).

Exigent circumstances is the only potentially relevant—and ultimately unavailing—warrant exception here. This exception “applies when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.” *Kentucky v. King*, 563 U.S. 452, 460 (2011) (internal quotation marks and brackets omitted). It has been held to permit “law en-

forcement officers [to] conduct a search without a warrant to prevent the *imminent* destruction of evidence.” *Missouri v. McNeely*, 133 S. Ct. 1552, 1559 (2013) (emphasis added). The potential destruction of evidence presents an exigent circumstance only where “there is compelling need for official action and no time to secure a warrant.” *Michigan v. Tyler*, 436 U.S. 499, 509 (1978).

2.1. REMOTE WIPE TECHNOLOGY DOES NOT AUTOMATICALLY ESTABLISH AN EXIGENT CIRCUMSTANCE.

Modern cell phones have a feature that enables the deletion of their contents remotely using another digital device. “Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data.” *Riley*, 134 S. Ct. at 2486. The existence of this feature on a phone is not nefarious or suspicious; it is simply standard.

This standard technological feature does not automatically give rise to an exigent circumstance on its own. The mere general capability for destruction does not give rise to exigency. The flammability of paper, for instance, does not automatically create an exigent circumstance in which to seize documents. Something more is required.

Case law from the analog context clarifies what must be shown to establish an exigent circumstance. The government's burden is discharged only when it presents concrete, particularized information suggesting that the destruction of evidence is imminent. For example, when the police are barricaded from entering a motel room by one occupant who tells the other to "get rid of the shit . . . flush the shit," an exigent circumstance arguably exists. *State v. Hall*, 555 So. 2d 495, 498 (La. Ct. App. 1989), *writ denied sub nom. State ex rel. Hall v. State*, 577 So. 2d 44 (La. 1991); *see also King*, 563 U.S. at 469-71 (exigency existed where suspects inside apartment react to police presence by hiding or destroying evidence).

Applying this standard to the digital context, courts overwhelmingly agree that the mere existence of a remote wipe feature does not give rise to an exigent circumstance. *See, e.g. U.S. v. Camou*, 773 F.3d 932, 941 (9th Cir. 2014); *U.S. v. Aispuro*, No. 13-10036-01, 2013 WL 3820017, at \*13 (D. Kan. July 24, 2013) (rejecting exigency because "[t]here was no specific evidence of such a threat in the instant case, although the Government's witnesses said loss of evidence was a concern"); *U.S. v. Jenkins*, No. 3:13-CR-30125-DRH-11, 2014 WL 2933192, at \*4 (S.D. Ill. June 30, 2014) (same) vacated in part on other grounds, No. 3:13-CR-30125-DRH-11, 2014 WL 4470609 (S.D. Ill. Sept. 10, 2014);

*U.S. v. Gomez*, 807 F. Supp. 2d 1134, 1145 n.13 (S.D. Fla. 2011) (“Objectively speaking, we find this concern unconvincing.”); *but see U.S. v. Zaavedra*, No. 12-CR-156-GKF, 2013 WL 6438981, at \*3 (N.D. Okla. Dec. 9, 2013) (holding that remote wipe feature established exigency, without discussion).

As the Supreme Court explained in *Riley*, remote wipe capabilities create exigency only where “police are truly confronted with a ‘now or never’ situation,—for example, circumstances suggesting that a defendant’s phone will be the target of an imminent remote-wipe attempt.” 134 S. Ct. at 2487 (quotations omitted) (emphasis added). Critically, there is simply no empirical evidence that criminal suspects’ cell phones are remotely wiped with any frequency. *See U.S. v. Wurie*, 728 F.3d 1, 11 (1st Cir. 2013) (“[T]he possibility of remote wiping here was ‘remote’ indeed.”), *cert. granted*, 134 S. Ct. 999 (2014) *and aff’d sub nom. Riley*, 134 S. Ct. 2473 (noting that there is “little reason” to believe remote wiping is prevalent).

2.2. REMOTE WIPE TECHNOLOGY DID NOT ESTABLISH AN EXIGENT CIRCUMSTANCE IN THIS CASE.

The Commonwealth argues that remote wiping “could . . . possibly” happen here. Br. Appellant at 23. But mere “possibility is simply not enough” to establish an exi-

gent circumstance, *U.S. v. Hayes*, 518 F.2d 675, 678 (6th Cir. 1975).

At bottom, the Commonwealth merely asserts that the suspect's cell phone might contain the same remote wipe feature as nearly every other modern cell phone. Raising the specter of remote wipe technology does not discharge the Commonwealth's burden of establishing exigency with *particularized* evidence of *imminent* evidence destruction. *See, e.g. Schlossberg v. Solesbee*, 844 F. Supp. 2d 1165, 1171 n.3 (D. Or. 2012) (rejecting exigency, though noting it might exist "where an officer had credible information that a suspect's accomplice was at a remote location and was planning to use Apple's remote-wipe program"). The Commonwealth's theory that co-conspirators could have initiated a remote wipe is equally speculative.

As logic and evidence suggest, and the decisions of other courts recognize, the mere fact that the owner of a cell phone with remote wipe technology participates in a joint criminal enterprise with others does not, in itself, give rise to exigent circumstances for seizing that person's cell phone. The Commonwealth has failed in this case to meet its burden of showing an exigent circumstance. Thus, law enforcement was required to obtain a warrant before seizing the defendant's cell phone. They failed to do so, thereby violating Article 14 and the Fourth Amendment.

3. IF A CELL PHONE IS SEIZED, THE FOURTH AMENDMENT  
REQUIRES THAT A WARRANT TO SEARCH IT MUST BE OBTAINED  
WITHOUT UNDUE DELAY.

Even a lawful seizure does not remain indefinitely so without a warrant. “[A] seizure reasonable at its inception because based on probable cause may become unreasonable as a result of its duration.” *Segura v. U.S.*, 468 U.S. 796, 812 (1984). “After seizing an item without a warrant, an officer must make it a priority to secure a search warrant that complies with the Fourth Amendment. This will entail diligent work to present a warrant application to the judicial officer at the earliest reasonable time.” *U.S. v. Burgard*, 675 F.3d 1029, 1035 (7th Cir. 2012), *cert. denied*, 133 S. Ct. 183 (2012). “When officers fail to seek a search warrant, at some point the delay becomes unreasonable and is actionable under the Fourth Amendment.” *Id.* at 1032; *see also U.S. v. Mitchell*, 565 F.3d 1347, 1350 (11th Cir. 2009) (quoting *U.S. v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998)); *Respress*, 9 F.3d at 488; *U.S. v. Dass*, 849 F.2d 414, 415 (9th Cir. 1988).

Although the Supreme Court has not dictated a bright line duration past which delays are per se unreasonable, it has required that courts weigh “the nature and quality of the intrusion on the individual’s Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.”

*Place*, 462 U.S. at 703; see also *Burgard*, 675 F.3d at 1033. In performing this weighing, courts examine (1) “the significance of the interference with the person’s possessory interest,” (2) “the duration of the delay,” (3) “whether or not the person consented to the seizure,” and (4) “the government’s legitimate interest in holding the property as evidence.” *U.S. v. Laist*, 702 F.3d at 613-14 (11th Cir. 2012). Given the high possessory interest cell phone owners have in their devices, lengthy delays cannot be tolerated in the absence of consent.

3.1. TOLERANCE FOR DELAY WHEN APPLYING TO SEARCH A COMPUTING DEVICE IS ESPECIALLY LOW.

When the police seize an individual’s computing device, the weight of the person’s possessory interest is “particularly powerful.” *Laist*, 702 F.3d at 613-14. An individual’s possessory interest in a computing device stems not only from physical repossession of his property, but also from the privacy rights implicated in maintaining access to his information. “The purpose of securing a search warrant soon after a suspect is dispossessed of a [container] . . . is to ensure its prompt return . . . If anything, this consideration applies with even greater force to the hard drive of a computer, which ‘is the digital equivalent of its owner’s home, capable of holding a universe of private in-



formation.’” *Mitchell*, 565 F.3d at 1352 (internal citations omitted). For cell phones, these possessory and privacy interests are at least as strong, if not stronger, as the Supreme Court recognized in *Riley*.

Although courts have allowed short delays in obtaining a warrant to search a legally seized electronic devices, *see, e.g., Commonwealth v. Kaupp*, 453 Mass. 102, 107, (2009) (permitting a 9-day delay, but suppressing evidence for lack of probable cause); *Burgard*, 675 F.3d at 1032 (permitting a 6-day delay), they have found even slightly longer delays amounting to less than a month to be unreasonable, *see, e.g., Mitchell*, 565 F.3d at 1350 (21-day delay after seizing a hard drive was unreasonable). This reflects the understanding that it should not take police officers several weeks to begin applying for search warrants for the cell phones they seize. *See id.* at 1347.

Probable cause either exists at the time a cell phone is seized, or it does not. If no probable cause exists, the seizure was unlawful *ab initio*, and no amount of evidence subsequently gathered evidence can retrospectively create the probable cause that was lacking at the time. *See Respress*, 9 F.3d at 486. If probable cause does exist, law enforcement must promptly seek judicial confirmation of that fact by applying for a warrant. Either way, such a lengthy delay as that at issue in this case is untenable.

3.2. WITHOUT A DEFENDANT’S CONSENT TO A SEIZURE, LONG DELAYS IN OBTAINING A WARRANT ARE NOT REASONABLE.

The Commonwealth cites to several cases in which long delays have been tolerated before searching computers, but each of those cases rests on a consensual seizure.<sup>3</sup> Br. Appellant at 30-31. This is important because “[w]hether or not the person consented to the seizure” weighs in determining the reasonableness of the delay. *Laist*, 702 F.3d at 613-14. Consequently, consent may authorize a delay whose length may otherwise be unacceptable.

For example, in *Laist*, a 25-day delay was held reasonable where the defendant signed consent forms authorizing the search and seizure of his computer. *Id.* at 616. In *People v. Shinohara*, the defendant again knowingly and voluntarily consented to a search. 375 Ill. App. 3d 85, 90 (2007). In *U.S. v. Stabile*, the court found that the defendant’s cohabitant had signed a consent form allowing investigators to take hard

---

<sup>3</sup> In its brief, the Commonwealth incorrectly cites *U.S. v. Jarman*, 61 F. Supp. 3d 598 (M.D. La. 2014), as holding that “delay of over a year in obtaining warrant [was] reasonable under circumstances presented.” Br. Appellant at 31. In fact, *Jarman* says the opposite. Seeing “no evidence that [the defendant] consented to the seizure or even knew that the seizure of the hard drive had occurred,” the court ultimately concluded that the “yearlong, warrantless seizure” was unreasonable. *Jarman*, 61 F. Supp. 3d at 603, 607.

drives from their residence. 633 F.3d 219, 233 (3d Cir. 2011).

These cases are inapposite here, where there is no evidence that the defendant consented to the seizure. Without consent, such a lengthy, warrantless seizure is not constitutionally permissible. There is no evidence here that the defendant consented to the seizure.

3.3. A 68-DAY DELAY BETWEEN SEIZING A CELL PHONE AND SEEKING A WARRANT CONSTITUTES UNDUE DELAY.

Warrant applications can be completed within a matter of days, if not less. *See Mitchell*, 565 F.3d at 1347. In *Mitchell*, an investigating officer who seized a hard drive without a warrant failed to submit a warrant application in the three days before he left town for a two-week training session. *Id.* The court held that the resulting 21-day delay in seeking a warrant was unreasonable. Even in *Burgard*, where a several-day delay was held reasonable, the court noted: “It strikes us as implausible that an officer with over 14 years of experience . . . could not write a two-page [warrant application] in fewer than six days.” 675 F.3d at 1034.

In the present case, officers took not six but 68 full days to apply for a search warrant. *Commonwealth v. White*, Mass. Super. Ct., No. 10-10511, slip op. at 3 (May 23, 2014). The detective who finally submitted the warrant application had 23 years of experience and had

“investigated or assisted in the investigation of over 1500” violent crimes. Aff. of Det. David Munroe at 1. It is difficult to believe that he required 10 weeks to draft a warrant application.

It is not sufficient that a warrant was eventually obtained, after the delay. “When an officer waits an unreasonably long time to obtain a search warrant, in violation of the Fourth Amendment, he cannot seek to have evidence admitted simply by pointing to that late-obtained warrant . . . In the line of Supreme Court decisions on which we have relied, the question is not whether police ultimately obtained a warrant; it is whether they failed to do so within a reasonable time.” *Burgard*, 675 F.3d at 1035. For the police to sit on a seized cell phone for over two months, waiting for probable cause to develop, is to bypass the requirement of having probable cause at the time of the seizure.

### CONCLUSION

*Amici* respectfully urge this Court to affirm the motion judge’s determination that the Commonwealth seized the defendant’s cell phone without probable cause, absent exigent circumstances, and that its failure to seek a warrant for ten weeks thereafter was patently unreasonable under Article 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution.

Respectfully submitted,  
American Civil Liberties Union of Massachusetts

BY THEIR COUNSEL<sup>4</sup>



Vivek Krishnamurthy (BBO No. Pending)  
1585 Mass Ave., Suite 5018  
Cambridge, MA 02138  
Tel: (617) 495-7547  
Fax: (617) 495-7641  
vkrishnamurthy@cyber.law.harvard.edu

Dated: November 23, 2015

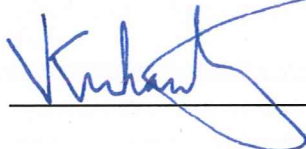
---

<sup>4</sup> *Amici* thank Harvard Law School Cyberlaw Clinic students Kenneth Monroe and Brian Pilchik for their valuable contributions to this brief.

### CERTIFICATE OF COMPLIANCE

I, Vivek Krishnamurthy, hereby certify pursuant to Mass. R. App. P. 16(k) that the instant 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), (b), (e), (f), and (h), 17, 18, and 20.

Dated: November 23, 2015



---

## **ADDENDUM**

### **CONSTITUTION OF THE UNITED STATES OF AMERICA AMENDMENT IV**

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

### **CONSTITUTION OF THE COMMONWEALTH OF MASSACHUSETTS ARTICLE XIV**

Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

## CERTIFICATE OF SERVICE

I, Vivek Krishnamurthy, hereby certify that on November 23, 2015, I caused two true and correct copies of the above document to be served on counsel of record for each other party by mailing the document by first-class mail, postage pre-paid, to the following:

### **Counsel for the Commonwealth**

Cailin M. Campbell  
Assistant District Attorney  
For the Suffolk District  
BBO No. 676342

One Bulfinch Place  
Boston, MA 02114  
617-619-4082  
cailin.campbell@state.ma.us

### **Counsel for Onyx White**

J.W. Carney, Jr.  
BBO No. 683134

Carney & Associates  
20 Park Plaza - Suite 1405  
Boston, MA 02116  
617-933-0350  
jcarney@carneydefense.com

Dated: November 23, 2015

