

No. _____

IN THE
Supreme Court of the United States

JAMES KEOWN,

Petitioner

v.

COMMONWEALTH OF MASSACHUSETTS,

Respondent

**Petition for Writ of Certiorari
to the
Supreme Judicial Court for the
Commonwealth of Massachusetts**

Counsel of Record for Petitioner

Claudia Leis Bolgen
Bolgen & Bolgen
110 Winn Street,
Suite 204
Woburn, MA 01801
(781) 938-5819
claudialb@bolgenlaw.com

Question Presented for Review

Whether a search warrant authorizing a search of all the files on a digital device is a general warrant lacking particularity under the Fourth Amendment unless *ex ante* search protocols are imposed in order to protect people's legitimate expectation of privacy from overreaching governmental intrusion into their most sensitive digital information.

List of Parties

The parties before the Court are James Keown and the Commonwealth of Massachusetts.

The parties before the Massachusetts Supreme Judicial Court were James Keown and the Commonwealth of Massachusetts.

Table of Contents

Question Presented for Review	ii
List of Parties	iii
Table of Contents	iv
Index to the Appendix	vi
Table of Authorities	vii
Petition for Writ of Certiorari	1
Citations to the Opinions Below	1
Statement of Jurisdiction	1
Relevant Constitutional and Statutory Provisions	1
Introduction	2
Concise Statement of the Case	3
<i>Facts Material to Consideration of Questions Presented</i>	3
Reasons for Granting the Petition	5
This Court should decide the important issue of whether the Fourth Amendment’s particularity requirement demands the imposition of <i>ex ante</i> search protocols prior to the search of all the files in a digital device, which could contain information about a person’s entire life.	5
A. The Massachusetts Supreme Judicial Court was wrong to reject <i>ex ante</i> restrictions on search warrants for digital searches.	10
B. The decision of the Massachusetts Supreme Judicial Court conflicts with the framework of analysis in this Court’s digital privacy decisions.	14

C.	The decision of the Massachusetts Supreme Judicial Court conflicts with the decisions of other courts on the question of <i>ex ante</i> search protocols.	16
D.	This Court must lead the way in protecting the privacy rights of citizens to the information contained in their digital devices.	21
Conclusion		24

Index to the Appendix

Opinion in <i>Commonwealth v. James Keown</i> , 478 Mass. 232, 84 N.E.3d 820 (2017)	1a
Search Warrant for a Sony VAIO laptop computer issued on June 8, 2006	17a
Opinion of the Middlesex Superior Court dated March 25, 2008	38a

Table of Authorities

CASES

<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987)	15
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	15
<i>Carpenter v. United States</i> , No. 16-402	15, 21
<i>Commonwealth v. James Keown</i> , 478 Mass. 232, 84 N.E.3d 820 (2017) ..	1
<i>Dalia v. United States</i> , 441 U. S. 238 (1979)	22
<i>In re Black iPhone 4</i> , 27 F. Supp. 3d 74 (D.D.C. 2014)	18, 19
<i>In re Cellular Telephones</i> , No. L4-MJ-8017-DJW, 2014 WL7793690 (D. Kan. Dec. 30, 2014)	18
<i>In re Nextel Cellular Tel.</i> , No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014)	18
<i>In re Search of 3817 W. West End</i> , 321 F. Supp. 2d 953 (N.D. Ill. 2004)	11, 16
<i>In re Search of Apple iPhone, IMEI 013888003738427</i> , 31 F. Supp. 3d 159 (D.D.C. 2014)	13, 18-20
<i>In re Search of Odys Loox Plus Tablet</i> , 28 F. Supp. 3d 40 (D. D.C. 2014)	18
<i>In re Search of premises known as Three Cellphones & One Micro-SD Card</i> , No. L4-MJ-8013-DJW, 2014 WL 3845157 (D. Kan. Aug. 4, 2014) .	18
<i>In re Search Warrant</i> , 71 A.3d 1158 (Vt. 2012)	16, 23
<i>In re U.S.'s Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius</i> , 770 F. Supp. 2d 1138 (W.D. Wash. 2011)	8, 9, 16
<i>In re [REDACTED]@gmail.com</i> , 62 F. Supp. 3d 1100 (N.D. Cal. 2014) ..	16

<i>Matter of the Search of Apple iPhone</i> , 31 F. Supp. 3d 159 (D.D.C. 2014)	19
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	5-7, 10, 14, 15, 23, 24
<i>United States v. Brooks</i> , 427 F. 3d 1246 (10 th Cir. 2005)	16
<i>United States v. Cartier</i> , 543 F.3d 442 (8 th Cir. 2008)	16
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9 th Cir. 2010)	12
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	12
<i>United States v. Ganas</i> , 824 F.3d 100 (2 nd Cir. 2016)	6
<i>United States v. Gourde</i> , 440 F.3d 1065 (9th Cir. 2006)	9
<i>United States v. Grubbs</i> , 547 U.S. 90 (2006)	22
<i>United States v. Hill</i> , 459 F. 3d 966 (9th Cir. 2006)	16
<i>United States v. Jones</i> , 132 S. Ct 945 (2012)	14, 15
<i>United States v. Microsoft</i> , No. 17-2	21
<i>United States v. Phua</i> , 2015 WL 1281603 (D. Nev. 2015)	13, 18, 19
<i>United States v. Richards</i> , 65 F.3d 527 (6 th Cir. 2011)	17
<i>United States v. Schesso</i> , 730 F.3d 1040 (9th Cir. 2013)	11, 16
<i>United States v. Ulbricht</i> , 858 F.3d 71 (2 nd Cir. 2017)	17

CONSTITUTIONAL PROVISIONS AND AUTHORITIES

2 <i>Legal Papers of John Adams</i> (1965)	11
Adam M. Gershowitz, <i>The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches</i> , Vanderbilt L. Rev. 69:3, at 598 (Apr. 2016)	10, 13

Monica Anderson, <i>Technology Device Ownership: 2015</i> , Pew Res. Ctr. (Oct. 29, 2015), available at http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/ (accessed Dec. 26, 2017)	9
<i>Most popular daily online activities of adult internet users in the United States as of February 2017</i> , (March 2017) available at https://www.statista.com/statistics/266891/daily-digital-activities-of-us-internet-users/ (accessed Dec. 26, 2017)	9
Paul Ohm, <i>Massive Hard Drives, General Warrants and the Power of Magistrate Judges</i> , 97 Va. L. Rev. Brief 1 (2011)	7, 23, 24
<i>The Law Dictionary (Featuring Black’s Law Dictionary Free Online Legal Dictionary 2nd Ed.)</i>	8
U.S. Const., amend. IV.	5
Victoria Barrett, <i>Dropbox: The Inside Story of Tech's Hottest Startup</i> , forbes.com (Oct. 18, 2011, 8:30AM), available at https://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/#5b0d38ff6437 (accessed December 26, 2017)	8

Petition for Writ of Certiorari

Petitioner James Keown (“Mr. Keown”) respectfully petitions for a writ of certiorari to the Massachusetts Supreme Judicial Court in this case.

Citations to the Opinions Below

The opinion of the Massachusetts Supreme Judicial Court (App. 1a-16a) is reported as *Commonwealth v. James Keown*, 478 Mass. 232, 84 N.E.3d 820 (2017).

Statement of Jurisdiction

The Massachusetts Supreme Judicial Court issued its opinion in this case on October 23, 2017. (App. 1a). Neither party petitioned that court for a rehearing. This Court has jurisdiction pursuant to 28 U.S.C. § 1257(a).

Relevant Constitutional and Statutory Provisions

United States Constitution Fourth Amendment

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.

Introduction

Searches of digital devices – in this case a laptop computer – are very different from searches of physical spaces. So, Fourth Amendment protections for such searches must be different as well.

The main differences between searches of digital devices and those of physical spaces are the amount of information at issue and the manner in which that information is stored. The unique features of digital devices make the application of the particularity requirement of the Fourth Amendment difficult using case law developed for physical spaces. Because of the vast volume of information contained in digital devices and the ever-evolving forensic tools available to comb through it, government overreach is both especially intrusive and increasingly avoidable when it comes to searches of digital devices. It is therefore of pressing importance that this Court implement new procedural safeguards to ensure that Fourth Amendment protections are effectively applied in the digital context.

Ex ante search protocols are the best way to implement the particularity requirement in the digital search context. They are constitutionally permissible, can be easily adapted to each particular case, and will assure judicial officials who issue search warrants that a search will be limited as much as possible to the information with respect to which probable cause has been established. This Court should implement *ex ante*

search protocols to preserve Fourth Amendment protections in this digital age.

Concise Statement of the Case

Mr. Keown was convicted by a jury on July 2, 2008 of murder in the first degree of his wife Julie Keown (“Julie”) by ethylene glycol poisoning. (App. 8-9a).

Facts Material to Consideration of Questions Presented

At trial, the Commonwealth sought to prove that a Sony VAIO laptop was primarily used by Mr. Keown. (T13:76).¹ A computer forensics expert found numerous Google searches for poisons and a search done on August 18, 2004 for “antifreeze death human” on the Sony VAIO. (T9:213-214). No poison Google searches were found on other laptops used by the couple. (T11:16-20).

The search warrant authorizing the forensic search of the Sony VAIO laptop by its terms envisioned a general search, not limited by protocols or keywords. The warrant allowed search of the entire laptop computer for the specific files referenced in 47(a)-(k) of the warrant application. “I seek permission to seize the....Sony Vaio....and search for the following electronic files:” (App. 30a). Paragraph (f) of the warrant application provided for a search of “any electronic file paper document specifically pertaining to the

¹The trial transcript will be cited as (“T [volume]:[page]”) and the transcript of the hearing on the motion to suppress as (“MTS:[page]”).

Internet activity of Keown.” (App. 31a). This paragraph purported to be limited to “computer files of the type described in Paragraph 2 of this affidavit.” (App. 31a). However, paragraph 2 of the affidavit simply described the Sony VAIO laptop and the hard drive and did not in any way concern types of computer files. (App. 20a). Thus, the four corners of the affidavit requested a general search of all the files contained on the entire laptop.

In addition, the actual search of the Sony VAIO laptop was done using keywords that were compiled prior to the warrant application but not submitted in the warrant application, as well as keywords added by prosecutor and the computer examiner after the warrant was issued. (MTS3:95-96). It is undisputed that the search terms ultimately used to search the Sony VAIO were not separately provided to a judge when police applied for a search warrant. (MTS4:36).

Prior to trial, Mr. Keown brought a motion to suppress evidence obtained from the search of the laptop computer on the basis that the warrant failed to describe the items to be seized with sufficient particularity. (App. 9a). This motion was denied. (App. 9a). On appeal to the Massachusetts Supreme Judicial Court, Mr. Keown again argued that the search warrant for the laptop lacked particularity and thus was an impermissible general warrant under the Fourth Amendment. (App. 9a). Specifically, Mr. Keown argued that an *ex ante* search protocol was

necessary in order to make a digital search warrant comport with the particularity requirement of the Fourth Amendment. (App. 10-11a). “While recognizing that the searches of electronic devices present major constitutional hazards” and citing to this Court’s decision in *Riley v. California*, 134 S. Ct. 2473, 2489-2490 (2014), the Massachusetts Supreme Judicial Court nevertheless declined to adopt *ex ante* search protocols for searches of electronic devices. (App. 10-11a). The only reasoning provided for this conclusion was that because the search was conducted reasonably and took place more than a decade ago, the laptop computer warrant did not lack particularity because it did not include *ex ante* search protocols. (App. 11a).

Reasons for Granting the Petition

This Court should decide the important issue of whether the Fourth Amendment’s particularity requirement demands the imposition of *ex ante* search protocols prior to the search of all the files in a digital device, which could contain information about a person’s entire life.

The Fourth Amendment to the United States Constitution requires that a warrant identify with particularity the place to be searched and the items to be seized. U.S. Const., amend. IV. This Court has recognized that the Fourth Amendment applies differently to searches of digital devices than to searches of physical places. See *Riley*, 134 S. Ct. at 2484-85. And this Court has also recognized that the pervasiveness of digital devices in people’s lives and the amount of information contained therein necessitates

more Fourth Amendment protections, not fewer. See *id.* It is the responsibility of this Court to formulate new Fourth Amendment rules for a new digital age, and to do so soon.

Applying the Fourth Amendment to searches of digital devices using past case law designed for physical spaces is difficult for five main reasons.

1. **Digital devices cannot be analogized to physical spaces.**

Case law concerning physical spaces, the foundation on which Fourth Amendment law has been based, simply isn't directly applicable to searches of digital devices. See e.g. *United States v. Ganius*, 824 F.3d 100, 212-215 (2nd Cir. 2016)(en banc)(analyzing the differences between digital and physical spaces). Electronic files “are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files” but rather are “fragmented” on the device. *Id.* at 213. In addition, electronic devices store not only files, but additional information about a given file, including metadata about the file's authorship and creation, and prior versions of the file. *Id.*

2. **Digital devices play a unique and unprecedented role in people's lives and society at large.**

This Court recognized the uniqueness of digital devices compared to anything ever seen previously when it pointed out that “[a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form – unless the phone is.” *Riley*, 134 S. Ct. at 2491. A laptop

– small, portable, ubiquitous and capable of storing many terabytes of information – is fully equivalent to a smartphone in this regard.

3. **Digital devices contain extremely large quantities of information.**

Digital devices contain vastly larger amounts of information than a typical house could even hold. See *Riley*, 134 S. Ct. at 2491, 2493 (search of a phone would “typically expose to the government far more than the most exhaustive search of a house.”). The Library of Congress contains ten terabytes of information, which will be the size of an average hard drive in the near future. See Paul Ohm, *Massive Hard Drives, General Warrants and the Power of Magistrate Judges*, 97 Va. L. Rev. Brief 1, 4 (2011) (“*Massive Hard Drives*”) (noting the Library of Congress contains ten terabytes of information, the size of an average hard drive in approximately six years). The vastness of the storage potential of a typical computer hard drive leads to another problem, which is that one digital device can store information dating back many years. This situation allows an unfettered government search to conduct what amounts to an archeological dig into a user’s past.

4. **Digital devices contain many types of data that would not be found together in a physical space.**

In contrast to a physical storage space like a briefcase, pants pocket or a purse, a digital device stores location history, call logs, text messages, e-mail accounts, health records, financial records, appointments, search and

browser histories, personal files, contacts and directories, voice memoranda, photographs, and more. Computers can also function as points of seamless access to data on a remote server², which can further expand the range of information a law enforcement search of data could reach. If a computer or other device contains a Dropbox³ application, for instance, an unconstrained search on the device could allow law enforcement to view and collect all the information stored there.

5. Digital devices contain data that is different in kind than exists in physical spaces.

Whereas a search of a file cabinet or a wallet would reach items consciously put there by someone, computers collect and store data the user has not affirmatively chosen to download and save, for example, cache files, which are “files automatically stored on a user’s hard drive by a web browser to speed up future visits to the same websites, without the affirmative action of downloading”. *In re U.S.’s Application for a Search*

²A remote server is a "server that is dedicated to handling users that are not on a [local access network] but need remote access to it. The remote access server allows users to gain access to files and print services on the LAN from a remote location." *The Law Dictionary (Featuring Black’s Law Dictionary Free Online Legal Dictionary 2nd Ed.)*, available at <http://thelawdictionary.org/remote-server/> (accessed December 26, 2017).

³Dropbox is a digital storage service. Victoria Barrett, *Dropbox: The Inside Story of Tech’s Hottest Startup*, forbes.com (Oct. 18, 2011, 8:30AM), available at <https://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/#5b0d38ff6437> (accessed December 26, 2017).

Warrant to Seize and Search Electronic Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1145 (W.D. Wash. 2011). Similarly, once information is present on a digital device, it is difficult or impossible for a user to destroy or delete this information. See *id.* Unlike papers removed from a file cabinet and discarded, remnants of an electronic file routinely remain on a device even after the file has been deleted. See *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (noting that even deleted files leave a "digital footprint" on a computer). Because so many people use digital devices, it is a certainty that the vast majority of United States citizens have information on their digital devices which was placed there without their affirmative action and which they can not remove even if they were aware of it being there. As of 2015, approximately 73 percent of U.S. adults had a desktop or laptop; 68 percent had a smartphone; and 45 percent had a tablet. Monica Anderson, Technology Device Ownership: 2015, Pew Res. Ctr. (Oct. 29, 2015), available at <http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/> (accessed Dec. 26, 2017). This situation is especially problematic when combined with a government search because people use their digital devices in connection with the most intimate aspects of their lives, such as sending and receiving e-mails, finding information about goods and services, conducting banking transactions, seeking personal information, and more. See *Most popular daily online activities of adult internet users in the*

United States as of February 2017, (March 2017) available at <https://www.statista.com/statistics/266891/daily-digital-activities-of-us-internet-users/> (accessed Dec. 26, 2017).

As detailed above, the data on digital devices is more voluminous, of a more diverse type and serves a different function than items found in the physical world. Thus, digital devices call for greater Fourth Amendment protection than is extended to physical objects containing less or narrower kinds of data. Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, Vanderbilt L. Rev. 69:3, at 598 (Apr. 2016)(describing how particularity takes on more importance in the digital context).

A. The Massachusetts Supreme Judicial Court was wrong to reject *ex ante* restrictions on search warrants for digital searches.

The Massachusetts Supreme Judicial Court has seriously misinterpreted the Fourth Amendment as applied to searches of digital devices by rejecting the application of *ex ante* restrictions on search warrants for digital evidence. The Fourth Amendment “was the founding generation’s response to 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. Warrants allowing unconstrained rummaging searches of digital devices must be prohibited by the Fourth Amendment

because these are closely analogous to the reviled general warrants of Colonial times. See *Riley*, 134 S. Ct. at 2494. Writs of assistance sought by Crown officials in Boston in 1761 (center stage for controversial British search and seizure practices) were general standing warrants permitting entry to any house to search for smuggled goods. See 2 *Legal Papers of John Adams* 107-108 (1965). Searching was done with unlimited discretion and the customs official could go to any “Vaults, Cellars...or other Places” and open “any Trunks, Chests, Boxes, fardells or Packs” *Id.* at 134. The search of every file in a digital device is closely analogous to these Colonial-era unconstrained rummaging searches.

Given the huge amount of information on digital devices and the fragmented way it is stored, there is a high likelihood that data relevant to an investigation will be mixed with irrelevant data. See *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004). This situation poses an unacceptably large risk that investigators will feel entitled to open any file among the millions contained on a smartphone or computer hard drive. See *United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013) (recognizing the risk that “identifying seizable electronic evidence could become a vehicle for the government to gain access to a larger pool of data that it has no probable cause to collect”). Unlike searches in the physical realm, where an investigator could not search for a stolen large-screen television in a medicine cabinet, investigators can be tempted

to search every file on a digital device because the size or outward appearance of any file or folder may disclose nothing about its contents. See *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013)(limitations on what to search "are largely absent in the digital realm, where the size or other outwardly visible characteristics of a file may say nothing about its content").

Freedom to open any file on a device as a matter of routine cannot satisfy the Fourth Amendment's particularity requirement. To hold otherwise would make a nullity of the Fourth Amendment's prohibition on general warrants and exploratory rummaging. For this reason particularity in the digital context must receive this Court's special attention.

Courts have recognized that when law enforcement requests broad authorization to examine digital records this creates a serious risk that every warrant for digital information will become, in effect, a general warrant "rendering the Fourth Amendment irrelevant." See *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010). In a concurring opinion which is widely cited, Judge Kozinski suggested guidance to mitigate this concern which included that "the government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by case agents." *Id.* at 1180 (Kozinski, concurring). Search protocols are defined as an explanation of the methodology law enforcement will use to separate

what is permitted to be seized from what is not. See *In re Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014); *United States v. Phua*, 2015 WL 1281603 at *7 (D. Nev. 2015) (“A protocol for forensic review of a device that stores data electronically must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.”)

This Court should now implement the concept of *ex ante* search protocols in warrants for digital searches. The search warrant for the laptop in this case authorized the government to look at every file on the laptop, (App. 20a, 30-31a), and this Court should find that this was an impermissible general warrant. Judges, not police or civilian forensic examiners must be the decisionmakers on particularity.

Properly implemented, *ex ante* warrant restrictions are an effective tool to reduce the privacy invasion inherent in searches of digital devices. See Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585, 614-628 (2016). This Court must correct the Massachusetts Supreme Judicial Court’s erroneous interpretation of the Fourth Amendment and require that police

must show a judge a genuine effort to limit themselves to a particularized search before the issuance of a search warrant for a digital device.

B. The decision of the Massachusetts Supreme Judicial Court conflicts with the framework of analysis in this Court’s digital privacy decisions.

Digital searches are different. That was this Court’s message in *Riley v. California*, 134 S. Ct. at 2489-2491. The tremendous storage capacity of a digital device required a new Fourth Amendment rule. See *id.* at 2489. This Court also recognized that the sensitivity of the information contained in a digital device and the unprecedented role of digital devices in people’s lives demand extra Fourth Amendment protections for searches of digital devices. *Riley*, 134 S. Ct. at 2491; see also *United States v. Jones*, 132 S. Ct 945, 957 (2012)(Sotomayor, J. concurring)(questioning the viability of Fourth Amendment jurisprudence developed in the context of physical searches to the “digital age”). The same principles hold true in this case, but the Massachusetts Supreme Judicial Court did not apply them in its decision.

As this Court noted in *Riley*, any decision in favor of digital privacy will have an impact on the ability of law enforcement to combat crime. *Riley*, 134 S. Ct. at 2493. But digital devices containing “the privacies of life” demand special Fourth Amendment treatment in order to avoid the reviled “general warrant” that the Fourth

Amendment was enacted to eradicate. *Id.* at 2494-2495, quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886). "[T]here is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all." *Arizona v. Hicks*, 480 U.S. 321, 329 (1987). The relevant question is where to strike this balance. See *id.*

This Court has also concerned itself with digital privacy in the context of timeframe. See *United States v. Jones*, 132 S. Ct 945, 957 (2012)(Sotomayor, J. concurring)(doubting that people would accept disclosure to the Government of a list of every Web site they had visited in a year); see also *Carpenter v. United States*, No. 16-402 (certiorari granted to decide whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the expansive timeframe of 127 days is permitted by the Fourth Amendment). *Ex ante* search protocols would mitigate such issues by explaining how investigators would go about limiting searches to a relevant timeframe, when computers typically store years worth of material.

This Court should continue its protection of digital privacy in this case. Here, this Court has an opportunity to thoughtfully apply the Fourth Amendment to searches of digital devices and require search warrants for digital devices to include search protocols, defined

as an explanation of the methodology law enforcement will use to separate what is permitted to be seized from what is not.

C. The decision of the Massachusetts Supreme Judicial Court conflicts with the decisions of other courts on the question of *ex ante* search protocols.

Courts in the Tenth Circuit, the Ninth Circuit, the Eighth Circuit, and a number of federal district and state courts have all issued decisions finding or assuming search protocols to be permissible.⁴ Such courts have ruled that, while an *ex ante* protocol may not be required in every case, employment of such protocols is looked upon "favorably," *United States v. Hill*, 459 F. 3d 966, 978 (9th Cir. 2006), and may even be "essential . . . especially in cases involving record searches where nonresponsive information is intermingled with relevant evidence." *In re Search Warrant*, 71 A.3d 1158, 1184 (Vt. 2012).

There is, however, no national consensus on the issue of search protocols, as other courts have rejected the use of search protocols

⁴*United States v. Schesso*, 730 F.3d 1040, 1050 (9th Cir. 2013); *United States v. Cartier*, 543 F.3d 442, 447-48 (8th Cir. 2008); *United States v. Hill*, 459 F. 3d 966, 978 (9th Cir. 2006); *United States v. Brooks*, 427 F. 3d 1246, 1252 (10th Cir. 2005); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1103 (N.D. Cal. 2014); *In re U.S.'s Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1139, 1150, 1153 (W.O. Wash. 2011); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 961 (N.D. Ill. 2004); *In re Search Warrant*, 71 A.3d 1158, 1170 (Vt. 2012).

altogether.⁵ These courts appear to analogize the search of every file in a digital device to physical searches of a whole house or business when probable cause supports that the searched-for evidence can be found anywhere. See *United States v. Ulbricht*, 856 F.3d 71, 99 (2nd Cir. 2017). The problem with this reasoning is that digital devices are simply not comparable to a search of a residence for the five reasons set forth above. An unconstrained governmental rummage through a person's cellphone or laptop computer is much more intrusive – and more violative of Fourth Amendment rights – than any physical search could ever be. Another concern is the practical problem that investigators might not know the particular search terms in advance of the search and therefore should be able to open any file. See *United States v. Richards*, 659 F.3d at 538-540. But it is far from clear that *ex ante* restrictions will actually make forensic digital searches more difficult. When law enforcement can submit a proposed protocol in the first instance specific to the case at hand, and can come back later for expanded or different search authority if needed, enforcing the particularity requirement of the Fourth Amendment in this manner does not inordinately burden digital forensic analysts while protecting the privacy interests of individuals in their digital devices.

⁵See *e.g. United States v. Ulbricht*, 858 F.3d 71, 99 (2nd Cir. 2017); *United States v. Richards*, 65 F.3d 527, 538 (6th Cir. 2011).

Importantly, other courts have decided that *ex ante* protocols are not only permissible, but they are required in order to make sure that searches of digital devices pass Fourth Amendment muster. These decisions prioritize concerns about probable cause and particularity in conjunction with the unique volume and sensitivity of information implicated in digital searches, and therefore hold that investigators may assure courts of a warrant's particularity only by formulating *ex ante* protocols.⁶

Because technology gives investigators the ability to "find specific data without having to examine every file on a hard drive or flash drive," and the risk of abuse inherent in a cursory examination of many intermingled files is so great, investigators should and can provide the court a technical explanation of how they plan to determine the correct area of the digital device to examine. *In re Search of Apple iPhone*, 31 F. Supp. 3d at 167. The courts in this line of cases are concerned in large part with how the government will

⁶See *United States v. Wei Seng Phua*, No. 2:14-CR-00249-APG, 2015 WL 1281603 at *7 (D. Nev. Mar. 20, 2015); *In re Cellular Telephones*, No. L4-MJ-8017-DJW, 2014 WL7793690 (D. Kan. Dec. 30, 2014); *In re Search of premises known as Three Cellphones & One Micro-SD Card*, No. L4-MJ-8013-DJW, 2014 WL 3845157 (D. Kan. Aug. 4, 2014); *In re Nextel Cellular Tel.*, No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014); *In re Search of Apple iPhone*, IMEI 013888003738427, 31 F. Supp. 3d 159, 166 (D.D.C. 2014); *In re Search of Odys Loox Plus Tablet*, 28 F. Supp. 3d 40 (D. D.C. 2014); *In re Black iPhone 4*, 27 F. Supp. 3d 74 (D.D.C. 2014).

separate relevant from irrelevant material. See *id.* at 167 (requiring protocol that will explain how investigators will "help limit the possibility that locations containing data outside the scope of the warrant will be searched"); *In re Black iPhone 4*, 27 F. Supp. 3d 74, 79 (D.D.C. 2014) (holding that government "must explain how it will deal with the issue of intermingled documents"); *United States v. Phua*, 2015 WL 1281603 at *7 (D. Nev. 2015) ("A protocol for forensic review of a device that stores data electronically must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.").

A judicial officer does not need to be in a position to dictate forensic search methods, but he or she must be given sufficient information to decide whether the contemplated search is sufficiently particular to pass Fourth Amendment muster. See e.g. *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (not dictating that particular terms or search methods be used, but needing a "sophisticated technical explanation of how the government intends to conduct the search so that the Court may conclude that the government is making a genuine effort to limit itself to a particularized search"). Judges are now more than capable of dealing with sophisticated search protocols.

See *iPhone*, 31 F. Supp. 3d at 168 (“The government should not be afraid to use terms like ‘MD5 hash values,’ ‘metadata,’ ‘registry,’ ‘write blocking’ and ‘status marker,’ nor should it shy away from explaining what kinds of third party software are used and how they are used to search for particular types of data.”). And, judges do not have to create search protocols: they can ask that law enforcement submit proposed protocols. All that a judicial officer is evaluating is the government’s “sophisticated technical explanation” of how it will conduct the search. *Id.*

Investigators may also return to the court for additional authorization if needed, and the application need only make clear that the government has based its request, including its search methodology, upon the knowledge it had at the time of the request. *Id.* (stating that the government may return "as needed" to obtain additional search authorization, and "the application need only explain that some searches require additional techniques and that what is proposed is merely what the government intends to do at the time it submits its application") (emphasis omitted). When law enforcement can submit a proposed protocol in the first instance specific to the case at hand, and can come back later for expanded or different search authority if needed, enforcing the particularity requirements of the Fourth Amendment in this manner does not

inordinately burden digital forensic analysts while protecting the privacy interests of individuals in their digital devices.

D. This Court must lead the way in protecting the privacy rights of citizens to the information contained in their digital devices.

This Court should grant this petition in order to continue the process of bringing Fourth Amendment protections to bear on the current digital landscape. See e.g. *Carpenter v. United States*, No. 16-402 (certiorari granted to decide whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the expansive timeframe of 127 days is permitted by the Fourth Amendment); see also *United States v. Microsoft*, No. 17-2 (certiorari granted to decide whether a United States provider of email services must comply with a probable-cause-based warrant by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad).

Ex ante search warrant restrictions on digital searches can be authorized by three separate parts of the Fourth Amendment: (1) that warrants be based “upon probable cause”, (2) that warrants particularly describe the “place to be searched, and the persons or things to be seized” and (3) that searches and seizures be reasonable. *Ex ante* search restrictions of digital evidence are crucial to guarding

against a lack of probable cause and particularity **before** a search that violates the Fourth Amendment occurs.

It is time for this Court to move forward from its prior case law concerning the execution of physical-space searches in light of the five differences highlighted above between searches of digital devices and physical world searches. In *United States v. Grubbs*, 547 U.S. 90, 97-98 (2006) this Court set out a narrow definition of particularity that did not include any conditions precedent to the execution of a warrant. But *Grubbs* did not involve a computer search warrant; the case involved an anticipatory warrant for a physical package containing child pornography videotapes. *Id.* at 92. In *Dalia v. United States*, 441 U. S. 238, 257 (1979), this Court held that the Fourth Amendment does not require that search warrants include a specification of the precise manner in which they are to be executed. However, *Dalia* considered an order authorizing the interception of oral communications by means of a "bug" installed by the police in the petitioner's office, and the issue in dispute was whether the warrant had to specify execution by covert entry. *Id.* at 256-257. This factual situation is not applicable to the search of a massive computer hard drive, where the methodology used to determine how the hard drive will be searched for responsive data within the scope of the warrant merges so completely with the place to be searched. In contrast with the physical world searches in *Grubbs* and *Dalia*, the "where" and the

“how” of searching are the same thing when considering the search of a digital device. See *In re Search Warrant*, 71 A.3d at 1171, where the Supreme Court of Vermont found that “the only feasible way to specify a particular ‘region’ of the computer will be by specifying how to search.” This difference is critical because the particularity clause of the Fourth Amendment should be read differently for digital searches, as this Court has done for other aspects of the Fourth Amendment. See *Riley*, 134 S. Ct. at 2494-2495.

And, *ex ante* restrictions on computer search warrants are not primarily about the reasonableness of how a digital search is executed, which generally certainly can be evaluated by a court after the search. But *ex ante* search restrictions of digital evidence are mainly about guarding against a lack of probable cause and particularity in the first instance. See Paul Ohm, *Massive Hard Drives*, at 4. The sheer amount of information involved and its personal and sensitive nature is the difference here. See *Massive Hard Drives*, at 5-8. Allowing law enforcement to haul off a digital device to search through all of its files however law enforcement sees fit in order to find the few items for which the warrant establishes probable cause, leads to an utter failure of both probable cause and particularity. See *id.* Such problems cannot alone be rectified with an after-the-fact focus on “reasonableness”.

This case picks up where *Riley* left off. When in *Riley* this Court directed the government to “get a warrant”, *Riley*, 134 S. Ct. at 2495, now is the time to further define what sort of warrant this Court contemplated. Clearly this Court did not mean that a general warrant for an unmitigated rummage through as much information as held by the Library of Congress would suffice. See *Massive Hard Drives* at 4 (noting the Library of Congress contains ten terabytes of information, the size of an average hard drive in approximately six years). This Court should therefore decide whether before-the-fact search protocols approved by a judge issuing a search warrant for a digital device are required for such a warrant to meet the Fourth Amendment’s particularity requirement.

Conclusion

For the reasons set forth above, this Court should grant this petition for writ of certiorari.

Respectfully submitted,

JAMES KEOWN

By his attorney,

/s/ Claudia Leis Bolgen

Claudia Leis Bolgen

Bolgen & Bolgen

110 Winn Street, Suite 204

Woburn, MA 01801

(781) 938-5819

claudialb@bolgenlaw.com

Dated: January 17, 2018