

COPY

COMMONWEALTH OF MASSACHUSETTS

SUPREME JUDICIAL COURT

NO. SJC-10593

RECEIVED
SUPREME JUDICIAL COURT

JAN 23 2017

Commonwealth of Massachusetts, FOR THE COMMONWEALTH
FRANCIS V. KENNEALLY, CLERK

Appellee,

v.

James Keown,

Appellant.

On Appeal from a Judgment
by the Middlesex Superior Court

Brief of Amici Curiae
Massachusetts Association of Criminal Defense Lawyers,
Committee for Public Counsel Services,
American Civil Liberties Union of Massachusetts,
Center for Democracy & Technology, and
Electronic Frontier Foundation
in Support of Appellant James Keown

Chauncey B. Wood
(BBO# 600354)
WOOD & NATHANSON, LLP
50 Congress Street, Ste.
600
Boston, MA 02109
Tel.: 617.776.1851
Counsel for MACDL

Alexis L. Shapiro
(BBO# 633562)
Margaret L. Sullivan
(BBO# 691492)
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
Tel.: 617.570.1000
Fax.: 617.523.1231
Counsel for MACDL

Matthew R. Segal
(BBO# 654489)
Jessie J. Rossman
(BBO# 670685)
ACLU OF MASSACHUSETTS
211 Congress Street
Boston, MA 02110
Tel: 617-482-3170

Donald S. Bronstein
(BBO# 058600)
COMMITTEE FOR PUBLIC
COUNSEL SERVICES
44 Bromfield Street
Boston, MA 02108
Tel.: 617-910-5794

Of counsel:

Gregory T. Nojeim
CENTER FOR DEMOCRACY &
TECHNOLOGY
1401 K Street NW, Ste. 200
Washington, DC 20005
Tel.: 202-637-9800

Andrew Crocker
Stephanie Lacambra
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: 415-436-9333

Dated: January 23, 2017

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENTS

Pursuant to S.J.C. Rule 1:21, 437 Mass. 1303 (2002), *amicus curiae* the Massachusetts Association of Criminal Defense Lawyers states that it is an incorporated association formed exclusively for charitable, scientific, and educational purposes that has no parent corporations and does not issue any stock.

Amicus Curiae the American Civil Liberties Union of Massachusetts states that it does not have a parent corporation, does not have subsidiaries, and does not issue any stock.

Amicus curiae the Center for Democracy & Technology states that it does not have a parent corporation, does not have subsidiaries, and does not issue any stock.

Amicus curiae the Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

TABLE OF CONTENTS

	Page
CORPORATE DISCLOSURE STATEMENTS.....	i
ISSUE PRESENTED.....	1
INTEREST OF THE AMICI CURIAE.....	1
STATEMENT OF THE CASE AND THE FACTS.....	4
SUMMARY OF ARGUMENT.....	5
ARGUMENT.....	6
I. Digital Devices Are Protected from Unreasonable Search and Seizure under the Fourth Amendment and art. 14 to the Massachusetts Declaration of Rights Because They Occupy a Unique Position in People's Lives, Giving Rise to a Reasonable Expectation of Privacy.....	6
II. Ex-Ante Search Protocols Help Uphold Fourth Amendment Protections in the Digital Context.....	15
A. Ex-Ante Search Protocols Are an Effective Tool.....	15
B. Individual Privacy Interests Trump Any Inconvenience to Government Investigation.....	17
III. Courts Have Begun to Look More Favorably on Search Protocols.....	21
IV. Massachusetts Should Revisit Its Jurisprudence on This Issue.....	25
V. The Lack of Search Protocol in Appellant's Case Mandates Suppression of the Evidence.....	30
CONCLUSION.....	32

TABLE OF AUTHORITIES

Page (s)

Cases

<i>In re [REDACTED]@gmail.com,</i> 62 F. Supp. 3d 1100, 1103 (N.D. Cal. 2014)	22
<i>Andresen v. Maryland,</i> 427 U.S. 463 (1976)	17
<i>In re Black iPhone 4,</i> 27 F. Supp. 3d 74 (D.D.C. 2014)	23, 24
<i>City of Los Angeles, Calif. v. Patel,</i> 135 S. Ct. 2443 (2015)	3, 6
<i>Commonwealth v. Augustine,</i> 467 Mass. 230 (2014)	4, 7
<i>Commonwealth v. Broom,</i> 474 Mass. 486 (2016)	29
<i>Commonwealth v. Lett,</i> 393 Mass. 141 (1984)	30
<i>Commonwealth v. Dorelas,</i> 473 Mass. 496 (2016)	15, 27, 28
<i>Commonwealth v. McDermott,</i> 448 Mass. 750 (2007)	26, 28, 30
<i>Commonwealth v. White,</i> 475 Mass. 583 (2016)	29, 30
<i>Dalia v. United States,</i> 441 U.S. 238 (1979)	17
<i>Minnesota v. Carter,</i> 525 U.S. 83 (1998)	6
<i>In re Nextel Cellular Tel.,</i> No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014)	23
<i>Preventive Medicine Assocs. v. Commonwealth,</i> 465 Mass. 810 (2013)	27

<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	passim
<i>In re Search of 3817 W. West End</i> , 321 F. Supp. 2d 953 (N.D. Ill. 2004)	9, 13, 16, 22
<i>In re Search of Apple iPhone, IMEI</i> 013888003738427, 31 F. Supp. 3d 159, 168 (D.D.C. 2014)	21, 23, 24
<i>In re Cellular Telephones</i> , No. 14-MJ-8017-DJW, 2014 WL 7793690 (D. Kan. Dec. 30, 2014)	18, 21, 23
<i>In re Search of ODYS LOOX Plus Tablet</i> , 28 F. Supp. 3d 40 (D.D.C. 2014)	23
<i>In re Search of Premises Known as Three</i> <i>Cellphones & One Micro-SD Card</i> , No. L4-MJ-8013-DJW, 2014 WL 3845157 (D. Kan. Aug. 4, 2014)	9, 14, 23
<i>In re Search Warrant</i> , 193 Vt. 51 (2012)	18, 19, 22
<i>United States v. Brooks</i> , 427 F.3d 1246 (10th Cir. 2005)	22
<i>United States v. Cartier</i> , 543 F.3d 442 (8th Cir. 2008)	22
<i>United States v. Comprehensive Drug Testing</i> , 621 F. 3d 1162 (9th Cir. 2010)	16
<i>United States v. Filippi</i> , No. 5:15-CR-133 BKS, 2015 WL 5789846 (N.D.N.Y. Sept. 9, 2015)	22
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	14
<i>United States v. Ganas</i> , 824 F.3d 199 (2d Cir. 2015) (<i>en banc</i>)	8
<i>United States v. Garcia-Alvarez</i> , No. 14-CR-0621 JM, 2015 WL 777411 (S.D. Cal. Feb. 24, 2015)	22

<i>United States v. Gourde</i> , 440 F.3d 1065 (9th Cir. 2006)	12
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	22
<i>United States v. Mujahid</i> , No. 3:09-CR-00053-TMB, 2011 WL 3920212 (D. Alaska Sept. 7, 2011)	22
<i>United States v. Schesso</i> , 730 F.3d 1040 (9th Cir. 2013)	14, 22
<i>United States v. Wei Seng Phua</i> , No. 2:14-CR-00249-APG, 2015 WL 1281603 (D. Nev. Mar. 20, 2015)	23

Statutes, Regulations, and Laws

U.S. Const., amend. IV.....	<i>passim</i>
Mass. Decl. of Rights, art. 14.....	<i>passim</i>

Other Authorities

<i>Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section Criminal Division</i> , OLE EXEC. OFFICE FOR U.S. ATTORNEYS (2009), available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (accessed Jan. 17, 2017)	10, 21
Adam M. Gershowitz, <i>The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches</i> VANDERBILT L. REV. 69:3 (Apr. 2016)	15, 20
THE LAW DICTIONARY (FEATURING BLACK'S LAW DICTIONARY FREE ONLINE LEGAL DICTIONARY 2 ND ED.), available at http://thelawdictionary.org/remote-server/ (accessed Jan. 17, 2017)	11

INTERNET ACCESS – HOUSEHOLDS AND INDIVIDUALS: 2016, OFFICE FOR NATIONAL STATISTICS (Aug. 4, 2016), available at https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016 (accessed Jan. 17, 2017)	13
Monica Anderson, TECHNOLOGY DEVICE OWNERSHIP: 2015, PEW RES. CTR. (2015), available at http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/ (accessed Jan. 5, 2017)	12
<i>What’s Old Is New Again: Retaining Fourth Amendment Protections in Warranted Digital Searches (Pre-Search Instructions and Post-Search Reasonableness)</i> , NACDL FOURTH AMENDMENT ADVOCACY COMM., at 3 (May 18, 2014), available at http://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=33204&libID=33173 (accessed Jan. 17, 2017)	9
Victoria Barrett, <i>Dropbox: The Inside Story of Tech’s Hottest Startup</i> (Oct. 18, 2011, 8:30 AM), FORBES.COM, available at http://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/#45f5c8628639 (accessed Jan. 20, 2017)	11

ISSUE PRESENTED

Whether police lawfully searched the contents of Appellant's laptop computer, where the warrant lacked particularity and no ex-ante search protocol was used.

INTEREST OF THE AMICI CURIAE

The Massachusetts Association of Criminal Defense Lawyers ("MACDL") is the Massachusetts affiliate of the National Association of Criminal Defense Lawyers and an incorporated association representing more than 1,000 experienced trial and appellate lawyers who are members of the Massachusetts Bar and who devote a substantial part of their practices to criminal defense. The MACDL devotes much of its energy to identifying, and attempting to avoid or correct, problems in the Commonwealth's criminal justice system, including by filing *amicus curiae* briefs in cases raising questions of importance to the administration of justice.

The MACDL is invested in the result of this case because it will affect the rights of many MACDL clients. Digital device use is pervasive, and the protection of digital devices under the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights may be a

vital defensive tool in future cases. The MACDL can offer the Court its perspective on the unique role digital devices play in the lives of individuals and the strong interest those individuals have in protecting their digital devices' privacy under the Fourth Amendment and art. 14.

The Committee for Public Counsel Services ("CPCS"), the Massachusetts public defender agency, is statutorily mandated to provide counsel to indigent defendants in criminal proceedings. The issue raised in this case, concerning the need for reasonable proposed search protocols in applications for warrants to search digital devices, is of immediate importance to many of CPCS's clients, who may be subject to unreasonable and invasive searches of their digital devices in the absence of the requirement for such proposed search protocols.

It is in the interest of CPCS's clients and the fair administration of justice that CPCS's views be presented in order to contribute to this Court's full consideration of all aspects of the important issues raised in this case.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on

privacy and other civil liberties issues affecting the Internet, other communications networks, and associated and emerging technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty in the digital world.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 25 years. With roughly 33,000 active donors, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF has special familiarity with and interest in constitutional privacy issues that arise with new technologies, and has served as amicus in recent key Fourth Amendment cases including *City of Los Angeles, Calif. v. Patel*, 135 S. Ct. 2443 (2015), and *Riley v. California*, 134 S. Ct. 2473 (2014).

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 (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.

STATEMENT OF THE CASE AND THE FACTS

This case involves the search and seizure of information located on Appellant James Keown's laptop computer based on a warrant that was insufficiently particularized and thus unconstitutional.

The MACDL adopts the Statement of the Case and the Statement of the Facts that appear in Defendant-Appellant's Brief, Docket No. 23. The MACDL also adopts the facts pertaining to Appellant's motion to suppress as referenced at pages 24 to 26 of Defendant-Appellant's Brief.

SUMMARY OF ARGUMENT

Searches of digital devices—in this case, a laptop—are different from searches of physical spaces, both in the scale of information at issue and the way in which that information is stored. The unique features of digital devices and the enormous amount of information stored on them make Fourth Amendment and art. 14 protections all the more important to uphold, especially with respect to the particularity requirement. Given this volume of information and the tools available to comb through it, government overreach is both especially intrusive and increasingly avoidable when it comes to digital devices. It is therefore paramount that procedural safeguards be implemented to ensure that Fourth Amendment and art. 14 protections are effected in the digital context. *Infra* pp. 6-15.

Ex-ante search protocols are well-suited to this purpose. They are constitutionally permissible, and when formulated on a case-by-case basis, may assure magistrate judges that a search will be limited as much as possible to the information with respect to which probable cause has been established. Massachusetts should join the courts that have begun

to move toward ex-ante protocols to bolster Fourth Amendment protections. The Supreme Judicial Court should revisit its position on ex-ante protocols and implement them on a case-by-case basis to preserve Fourth Amendment and art. 14 protections in the digital context. *Infra* at 15-30.

Such search protocols were needed in this case, and because they were not used, the evidence seized from Appellant's laptop should have been suppressed. *Infra* at 30-32.

ARGUMENT

I. Digital Devices Are Protected from Unreasonable Search and Seizure under the Fourth Amendment and art. 14 to the Massachusetts Declaration of Rights Because They Occupy a Unique Position in People's Lives, Giving Rise to a Reasonable Expectation of Privacy.

The Fourth Amendment to the United States Constitution protects against unreasonable searches and seizures of persons, places, and effects when the person subject to the search or seizure has a legitimate expectation of privacy in the item searched or seized. *City of Los Angeles, Calif. v. Patel*, 135 S. Ct. 2443, 2451-52 (2015) (citing Fourth Amendment language protecting against unreasonable searches and seizures); *Minnesota v. Carter*, 525 U.S. 83, 88 (1998)

(holding that the ability to claim Fourth Amendment protection hinges on whether the person “has a legitimate expectation of privacy in the invaded place”) (internal quotations and citations omitted). To comply with the Fourth Amendment, a warrant must “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. Const., amend. IV.

The law is clear that people have a legitimate expectation of privacy in their digital devices. In *Commonwealth v. Augustine*, 467 Mass. 230 (2014), this Court held that the Fourth Amendment and art. 14 apply in full force to searches of cell phones. The Supreme Court also held as much regarding the Fourth Amendment in *Riley v. California*, 134 S. Ct. 2473 (2014), when it held that police were not entitled to a warrantless search of a person’s cell phone incident to arrest. The Court recognized that the pervasiveness of digital devices in people’s lives necessitated more Fourth Amendment protections, not fewer, than have traditionally extended to physical searches incident to arrest, which have been permitted on grounds of officer safety or destruction of evidence. *Id.* at 2484-85.

Digital devices can amplify Fourth Amendment interests for many reasons. First, they are not easily analogized to physical spaces, which are the foundation on which Fourth Amendment law has been based. See, e.g., *United States v. Ganius*, 824 F.3d 199, 216-18 (2d Cir. 2015) (*en banc*) (analyzing the differences between physical and digital spaces). For example, 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 214. 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.*

Digital devices also powerfully trigger Fourth Amendment protection because of the unique and unprecedented role they occupy in people’s lives and society at large. The *Riley* Court recognized the qualitative and quantitative singularity of digital devices 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.” 134 S. Ct. at 2491.

These concerns are not limited to smartphones, but rather are equally applicable to other digital devices, such as laptops, tablets, and computers.

As *Riley* recognized, digital information is different from other types of information both in scale and in kind. As an initial matter, a single digital device may hold far more information than any physical container likely to be searched. See *Riley*, 134 S. Ct. at 2491 (search of a phone would “typically expose to the government far more than the most exhaustive search of a house”); *In re Search of Premises Known as Three Cellphones & One Micro-SD Card*, No. L4-MJ-8013-DJW, 2014 WL 3845157, at *2 (D. Kan. Aug. 4, 2014) (requiring a search protocol because of the “large amounts of electronically stored information”); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) (citing the “extraordinary volume of information” that may be stored on a home computer); *What’s Old Is New Again: Retaining Fourth Amendment Protections in Warranted Digital Searches (Pre-Search Instructions and Post-Search Reasonableness)*, NACDL FOURTH AMENDMENT ADVOCACY COMM., at 3 (May 18, 2014), available at

<http://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=33204&libID=33173> (accessed Jan. 17, 2017)

("exponentially" more information may be found on a laptop or smartphone than in a cigarette case or briefcase). While a physical object generally stores only as much information as can feasibly fit in the object, electronic devices can enclose exponentially more information, despite being physically small.

Indeed, the measure of data on an average computer or smartphone will routinely rival or even outstrip the sum of information that law enforcement can locate in a conventional search of all the articles residing in a residence or office. *See Riley*, 134 S. Ct. at 2493.

And, beyond the sheer amount of data, a digital device may also contain many types of data. *See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section Criminal Division*, OLE EXEC. OFFICE FOR U.S. ATTORNEYS, § 2.C.2 (2009) (hereinafter "OLE EXEC. OFFICE"), available at

<https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf> (accessed Jan. 17, 2017). In contrast to a wallet or purse, for

example, 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 instant access to data on a remote server,¹ which can further expand the range of information a law enforcement search of data could reach. If a computer or other device contains a Dropbox² application, for instance, an unconstrained search on the device could allow law enforcement to view and collect all the information stored there.

Digital information is different in kind, as

¹ A 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 Jan. 17, 2017). For example, when an employee connects to his company's network from a home computer, he may be doing so through use of a remote server.

² Dropbox is a digital storage service. Victoria Barrett, *Dropbox: The Inside Story of Tech's Hottest Startup*, FORBES.COM (Oct. 18, 2011, 8:30 AM), available at <http://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/#45f5c8628639> (accessed Jan. 20, 2017).

well. For one, unlike in the context of physical spaces, computers download and save data the user has not affirmatively chosen to download and save (e.g., 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 Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1145 (W.D. Wash. 2011). Similarly, a user will usually only incompletely delete data from a digital device; unlike papers removed from a box in the home and discarded, remnants of an electronic file routinely remain on a device even after the file has been deleted. *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (noting that even deleted files leave a "digital footprint" on a computer). These distinctions matter, partly because so many people use digital devices. 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 Jan. 5, 2017). The distinct qualities of digital information are also significant 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 health-related information, and more. See INTERNET ACCESS - HOUSEHOLDS AND INDIVIDUALS: 2016, OFFICE FOR NATIONAL STATISTICS (Aug. 4, 2016), *available at* <https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016> (accessed Jan. 17, 2017).

These differences in function, size, and breadth of data stored on digital devices call for greater Fourth Amendment protection than is extended to physical objects containing less or narrower kinds of data. For instance, given the amount of information on digital devices and how it is stored there, 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 at 958 (collecting cases on need for particularity in digital

context because of amount of data and likelihood of intermingling). This intermingling creates a risk that investigators will feel entitled to open any file among the plethora contained on a smartphone or computer hard drive. See *United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013) (the court has recognized 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"); *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. Accordingly, particularity in the digital context must receive special attention. See, e.g., *In re Search of Premises Known as Three Cellphones and One Micro-SD Card*, 2014 WL 3845157, at *2 (holding that a protocol is required to determine

whether the government was executing its search with sufficient particularity in light of the unique characteristics of digital spaces); *Commonwealth v. Dorelas*, 473 Mass. 496, 502 (2016) (unique properties of digital devices require a search that meets “a more narrow and demanding standard”); 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) (hereinafter “Gershowitz”) (describing how particularity takes on more importance in the digital context).

II. Ex-Ante Search Protocols Help Uphold Fourth Amendment Protections in the Digital Context.

A. Ex-Ante Search Protocols Are an Effective Tool.

Ex-ante search protocols are an effective, lawful tool to diminish the heightened risks to Fourth Amendment rights in the digital search context. Such protocols render a search more particularized, obviating the need for investigators to rummage indiscriminately through intermingled documents for fear of missing relevant information. Moreover, the mere existence of such protocols may help assure the court that the government is working to tailor its search to the information sought. *See In re Search of*

3817 W. West End, 321 F. Supp. 2d at 955-56 (noting that purpose of protocol was to "provide the Court with assurance that the search of the computer would not consist merely of a random or general examination of other documents").

Ex-ante protocols can vary in design, with such design tailored to fit the facts of each individual case. As some examples, the court could require investigators to use an impartial party to conduct a search before transferring relevant files to investigators, to use keyword or date range parameters when searching, to limit their search to certain types of digital files, or to waive the plain view doctrine. See, e.g., *United States v. Comprehensive Drug Testing, Inc.*, 621 F. 3d 1162, 1178-79 (9th Cir. 2010) (Kozinski, J., concurring) (suggesting such methods as offering a "safe harbor" to investigators). The more specific limits will depend on the individual facts of a given case: specific accounts or apps to be searched (Facebook, Instagram, etc.), e-mail correspondence with specific actors (sender or recipient), file type limits (e.g., no downloading videos or photos if law enforcement has probable cause only for bank documents and call records), and file size limits (no

downloading bulk data to search later).

**B. Individual Privacy Interests Trump Any
Inconvenience to Government Investigation.**

Judicial officials may constitutionally impose ex-ante search protocols; indeed, protocols may be required by the Fourth Amendment in some cases. While “it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant,” *Dalia v. United States*, 441 U.S. 238, 257 (1979), it is well-established that judges “must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy.” *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). Such efforts on the part of a judicial official may involve engaging with investigators regarding “the place to be searched” as described by the Fourth Amendment. Ex-ante protocols allow judges to take these kinds of steps in connection with searches of digital devices, where the question of how to search blends together with the question of what will be searched. In the digital context, “physical notions of particularity” are “metaphorical at best”, and, often, “the way to

specify particular objects or spaces will not be by describing their physical coordinates but by describing how to locate them." *In re Search Warrant*, 193 Vt. 51, 70 (2012). In the digital arena, therefore, ex-ante protocols that determine how investigators will search are really a way of describing with particularity the location of the digital spaces and files that will be searched.

Further, despite critics' concerns to the contrary, ex-ante protocols do not replace or stunt the use of ex-post reasonableness reviews to determine the constitutionality of a search. Ex-ante protocols and ex-post review serve different purposes. Namely, ex-post review addresses harm incurred by an unconstitutional search and seizure, while ex-ante protocols seek prophylactically to avoid that constitutional injury. *See In re Cellular Telephones*, No. 14-MJ-8017-DJW, 2014 WL 7793690, at *10 (D. Kan. Dec. 30, 2014) (analyzing interaction between ex-ante and ex-post review while holding the government was required to submit a search protocol for approval). By limiting scrutiny of a search to ex-post reasonableness review, "the government not only possesses a substantial portion of an individual's

private life," but also leaves individuals vulnerable to unconstitutional searches, forcing them to defend their constitutional rights after the fact. *Id.* Ex-ante protocols have a separate, preventative function.

Critics also voice concern over whether judicial officials have sufficient technical expertise to properly implement ex-ante protocols. First, even without employing technical expertise, judges may require ex-ante protocols simply to assure themselves that investigators are using methods to tailor their search to the relevant materials. *See id.*, at *7-8 (noting that protocol "helps the court to determine if the proposed warrant satisfies the requirements of the Fourth Amendment"). For an ex-ante protocol to serve this purpose, a judge need not acquire particular technical expertise. And, in any event, investigators may explain technical issues for the judge at the time of application. *See In re Search Warrant*, 193 Vt. at 90 ("All the instruction calls for is that the persons conducting the search . . . educate the judicial officer on the need for these methods and obtain approval. . . . We [] believe that the judicial officer can be educated on the purpose and method of any search tool.").

Second, in the civil context, judicial officials regularly participate in technical discussions regarding discovery protocols for electronically stored information. For example, judges in civil matters regularly preside over disputes regarding discovery plans and motions to compel electronically stored information. See Gershowitz, at 625-26 (collecting cases). There is no reason judicial officials should not be able to participate in similar ways in a technical discussion in the criminal context.

Finally, critics have expressed concern that ex-ante protocols will unreasonably inhibit investigators in their searches and force them to conduct insufficient searches. For one, this criticism ignores the fact that ex-ante protocols should be formulated with the specific facts of each case in mind so as to reserve for investigators the leeway they need to locate evidence. It also discounts the iterative process investigators may engage in with judicial officials in implementing ex-ante protocols. If a search protocol initially approved by the judge does not allow for a sufficient search, investigators may return to the court to fine-tune the warrant. See *In*

re Search of Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, 168 (D.D.C. Mar. 26, 2014) (explaining that “the government can always return for additional authorization of this Court as needed”); *In re Cellular Telephones*, 2014 WL 7793690, at *10 (same).

The technology currently available to investigators also weighs against the argument that ex-ante protocols will always unreasonably constrain a search. Indeed, the government’s own internal guidance suggests the utility of protocols. See OLE EXEC. OFFICE, § 2.C.2 (warrant must describe the subject of the seizure with sufficient particularity and limit the description of what will be seized to the scope of probable cause established in the warrant; agents must “conduct narrow seizures that attempt to minimize unwarranted intrusions upon privacy”) (internal citations omitted).

III. Courts Have Begun to Look More Favorably on Search Protocols.

Recognizing the benefits of ex-ante search protocols and the fact that “digital is different” under *Riley*, courts are increasingly holding protocols in the digital setting to be permissible. Indeed, 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 protocols to be permissible.³ 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*, 193 Vt. at 90.

Other courts have gone even further, deciding that ex-ante protocols are *required* in the digital arena. Grounded in concerns about probable cause and

³ *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); *United States v. Filippi*, No. 5:15-CR-133 BKS, 2015 WL 5789846, at *5 (N.D.N.Y. Sept. 9, 2015); *United States v. Garcia-Alvarez*, No. 14-CR-0621 JM, 2015 WL 777411, at *4 (S.D. Cal. Feb. 24, 2015); *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.D. Wash. 2011); *United States v. Mujahid*, No. 3:09-CR-00053-TMB, 2011 WL 3920212, at *7 (D. Alaska Sept. 7, 2011); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 961 (N.D. Ill. 2004); *In re Search Warrant*, 193 Vt. 51, 65 (2012).

particularity in conjunction with the unique volume and sensitivity of information implicated in digital searches, these decisions hold that investigators may assure courts of a warrant's particularity only by formulating ex-ante protocols.⁴ Where, as in the digital search arena, 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 must 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 separate relevant from irrelevant material. *See, e.g., id.* at

⁴ *See United States v. Wei Seng Phua*, No. 2:14-CR-00249-APG, 2015 WL 1281603 (D. Nev. Mar. 20, 2015); *In re Cellular Telephones*, No. L4-MJ-8017-DJW, 2014 WL 7793690 (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 (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).

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”). Rather than “dictating that particular terms or search methods should be used,” these courts are “attempting to convey that [they want] a sophisticated technical explanation of how the government intends to conduct the search so that the [courts] may conclude that the government is making a genuine effort to limit itself to a particularized search.” *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168. A protocol should provide technical information to assure the court of the investigators’ efforts; investigators “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.” *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).

IV. Massachusetts Should Revisit Its Jurisprudence on This Issue.

Massachusetts courts have acknowledged the distinct nature of digital searches, and their jurisprudence on this issue continues to evolve. Nonetheless, unlike certain other jurisdictions, Massachusetts case law still does not require that investigators employ ex-ante search protocols in the digital setting, nor has any Massachusetts court even made clear that such protocols are permitted. This Court should revisit its thinking on digital searches and should require ex-ante protocols for the search of digital devices. The issuance of a warrant should not constitute a blank check to comb through all personal

digital information—regardless of relevance—stored on an individual’s digital device.

In the Commonwealth’s foundational case on this issue, *Commonwealth v. McDermott*, 448 Mass. 750 (2007), the Court rejected a challenge to the execution of a warrant to search the defendant’s computer. The defendant argued that the fruits of the search should be suppressed on the ground that the search had been “in an unreasonable manner” and that a “showing of probable cause” was required to search each file. *Id.* at 772, 777. Reasoning that, “[i]n conducting the actual search of the computers and disks, considerable discretion must be afforded to the executing officers regarding how best to proceed with the search,” the Court held that “[a]dvance approval for the particular methods to be used in the forensic examination of the computers and disks is not necessary.” *Id.* at 776. Though the Court went on to say that “care must be taken to minimize the intrusion of the search and [that] the search must be reasonable,” it also explicitly analogized the search of a digital device to that of a physical container. *Id.* at 771, 777. The Court concluded that the search at issue was reasonable, in part because the keyword

search method employed necessitated review of only 750 of the 100,000 files in the defendant's computer. *Id.* at 777.

Next, the Court decided *Preventive Medicine Assocs. v. Commonwealth*, 465 Mass. 810 (2013), in which it addressed the need for a search procedure specifically in the context of post-indictment e-mails by a "taint team" made up of individuals not involved with the investigation or prosecution of the defendant, to remove potentially privileged information from the document set before investigators could conduct a search. The Court held that the Commonwealth was required to seek judicial approval of the taint team's procedure prior to searching the post-indictment e-mails and noted that the Court "take[s] seriously the concern that a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment." *Id.* at 823, 831.

The Court continued its discussion of digital searches in January 2016 in *Commonwealth v. Dorelas*, 473 Mass. 496, in which it denied the defendant's motion to suppress but nonetheless continued to evolve in its treatment of digital evidence. The *Dorelas* defendant claimed that the evidence against him that

was found on his iPhone should be suppressed because there was not probable cause to search the photographs stored there. Unlike in *McDermott*, the Court in *Dorelas* discussed the large amount of information a person stores on an iPhone. Though the Court held the warrant had established probable cause in this case, it nonetheless held that, "given the properties that render an iPhone distinct from the closed containers regularly seen in the physical world, a search of its many files must be done with special care and satisfy *a more narrow and demanding standard.*" 473 Mass. at 502 & n.11 (emphasis added). For example, the Court stated that in the digital context, it is insufficient for investigators to limit their searches to anywhere the targeted objects could *possibly* be found, "as data possibly could be found anywhere within an electronic device" and "what might have been an appropriate limitation in the physical world becomes a limitation without consequence in the virtual one." *Id.* Moreover, the dissent in *Dorelas* advocated for even further privacy protections, and would require "particularized limitations beforehand for a search" where, as here, a digital device is being searched. *Id.* at 511. Both opinions recognized that the unique qualities of

digital information have implications for the Fourth Amendment and art. 14.

Last, in September 2016, the Court decided *Commonwealth v. White*, 475 Mass. 583 (2016), developing its jurisprudence about digital searches further still. In *White*, the Court held that when searching a digital device, the opinion of an investigating officer that people often use smartphones while committing crimes cannot alone provide the nexus between the crime and the device sufficient to establish probable cause.⁵ In so holding, the Court reiterated that individuals have “significant privacy interests” at stake in their digital devices and that the Fourth Amendment’s and

⁵ Amici note that this holding in *White* alone is sufficient to warrant reversal of the lower court’s decision to deny Appellant’s motion to suppress. The investigators’ warrant application relied solely upon the officer’s experience in how people generally use digital devices and failed to include any information establishing a nexus between this specific crime and this specific defendant, see R.A. 37, and thus falls squarely within *White*’s holding. See Reply Br. of the Defendant-Appellant at 12-15; see also *Commonwealth v. Broom*, 474 Mass. 486, 495, 52 N.E.3d 81, 89 (2016) (affidavit stating that affiant knew “from training and experience that cellular telephones contain multiple modes used to store vast amounts of electronic data, and that in his opinion” there was probable cause from that reason was “general” and “conclusory” and added “nothing to the probable cause calculus”) (internal quotations and citations omitted).

art. 14's probable cause requirements must protect those interests. *Id.* at 592 (internal quotations and citations omitted).

From *McDermott* to *White*, the Court increasingly recognized that digital searches present distinct and typically heightened concerns under the Fourth Amendment and art. 14. Given the Court's recognition that digital searches often deserve greater protections than searches of physical spaces, and given that ex-ante protocols are an effective, constitutionally permissible alternative to allowing under-particularized searches, the Court should hold that such protocols are required from investigators applying for a warrant to search digital devices.

V. The Lack of Search Protocol in Appellant's Case Mandates Suppression of the Evidence.

In Appellant's case, the investigators' warrant application and affidavit provided no indication of how they would seek to tailor their review to relevant information and avoid a review of all files, rendering it tantamount to a constitutionally impermissible general warrant, the fruits of which must be suppressed. See *Commonwealth v. Lett*, 393 Mass. 141, 145-46 (1984) ("It is beyond doubt that all evidence

seized pursuant to a general warrant must be suppressed.”) (emphasis and internal quotations and citations omitted). Though the officers used keywords to conduct their search, they provided no such terms in the warrant application itself, and thus failed to subject their methodology to judicial oversight. See R.A. at 24-41, 45. These deficits matter where, as here, investigators are searching for broad categories of information. The addendum to the warrant affidavit in this case contemplated a wide-sweeping search of files relating to Appellant’s wife’s health and/or death, electronic files related to poison, electronic files related to financial information, electronic files related to life insurance, electronic files related to preparation of a will, electronic files related to the Internet activity of Appellant, software used to perform data processing for financial information, software used to track calendar appointments, software used to encrypt, decrypt, or erase computer files, software that would be necessary to access or read any of the other items to be searched, and files showing the creation of, editing of, access to, and/or control of any of the other files to be searched. R.A. at 40-41. An unconstrained

search for such materials could easily lead investigators to personal and confidential but irrelevant information. Where technology allows investigators to avoid such general rummaging in violation of the Fourth Amendment and art. 14, they should be required to employ it in the form of an ex-ante search protocol appropriate to the facts of the particular case.

CONCLUSION

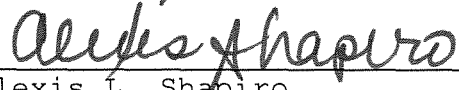
For these reasons, along with the reasons stated in the briefs of Appellant, amici curiae the Massachusetts Association of Criminal Defense Lawyers, Committee for Public Counsel Services, American Civil Liberties Union of Massachusetts, Center for Democracy & Technology, and Electronic Frontier Foundation respectfully request that this Court reverse the verdict below and grant Appellant a new trial, and rule that ex-ante search protocols are required from investigators applying for a warrant to search a digital device.

Respectfully submitted,

Dated: January 23, 2017

By their attorneys, .

Chauncey B. Wood
(BBO# 600354)
WOOD & NATHANSON, LLP
50 Congress Street, Ste.
600
Boston, MA 02109
Tel.: 617.776.1851


Alexis L. Shapiro
(BBO# 633562)
Margaret L. Sullivan
(BBO# 691492)
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
Tel.: 617.570.1000
Fax.: 617.523.1231
Counsel for MACDL

Matthew R. Segal
(BBO# 654489)
Jessie J. Rossman
(BBO# 670685)
ACLU OF MASSACHUSETTS
211 Congress Street
Boston, MA 02110
Tel: 617-482-3170

Donald S. Bronstein
(BBO# 058600)
COMMITTEE FOR PUBLIC COUNSEL
SERVICES
44 Bromfield Street
Boston, MA 02108
Tel.: 617-910-5794

Of counsel:


Gregory T. Nojeim
CENTER FOR DEMOCRACY &
TECHNOLOGY
1401 K Street NW, Ste.
200
Washington, DC 20005
Tel.: 202-637-9800

Andrew Crocker
Stephanie Lacambra
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: 415-436-9333

Counsel for Amici Curiae

MASS. R.A.P. 16(K) COMPLIANCE CERTIFICATION

I, Alexis L. Shapiro, hereby certify that the foregoing Brief of the Massachusetts Association of Criminal Defense Lawyers, Committee for Public Counsel Services, American Civil Liberties Union of Massachusetts, Electronic Frontier Foundation, and the Center for Democracy & Technology as Amici Curiae in Support of Appellant James Keown complies with the rules of court that pertain to the filing of briefs, including but not limited to Mass. R.A.P. 16(a) (contents of briefs); Mass. R.A.P. 16(e) (references to the record); Mass. R.A.P. 16(f) (reproduction of statutes, rules, regulations); Mass. R.A.P. 16(h) (length of briefs); Mass. R.A.P. 17 (amicus briefs); Mass. R.A.P. 18 (appendix to briefs); and Mass. R.A.P. 20 (form of briefs, appendices, and other papers).


Alexis L. Shapiro

CERTIFICATE OF SERVICE

I, Alexis L. Shapiro, counsel for Amicus Curiae Massachusetts Association of Criminal Defense Lawyers, hereby certify that I have served two copies of this Brief of the Massachusetts Association of Criminal Defense Lawyers, Committee for Public Counsel Services, American Civil Liberties Union of Massachusetts, Electronic Frontier Foundation, and the Center for Democracy & Technology as Amici Curiae in Support of Appellant James Keown by causing them to be delivered by first-class mail, postage prepaid, to counsel of record at the following addresses this 23rd day of January, 2017.

Marian T. Ryan
Jamie Michael Charles
Office of the Middlesex
District Attorney
15 Commonwealth Avenue
Woburn, MA 01801

Claudia Leis Bolgen, Esq.
Bolgen & Bolgen
110 Winn Street, Ste. 204
Woburn, MA 01801


Alexis L. Shapiro