

COMMONWEALTH OF MASSACHUSETTS

APPEALS COURT

Worcester County

No. 2005-P-0375

COMMONWEALTH OF MASSACHUSETTS,
Appellee,

v.

MICHAEL E. BRYANT,
Appellant

On Appeal from Judgments of the Superior Court

BRIEF OF *AMICI CURIAE*
NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN AND
AMERICAN PROSECUTORS RESEARCH INSTITUTE
IN SUPPORT OF APPELLEE

BERKMAN CENTER FOR
INTERNET AND SOCIETY
HARVARD LAW SCHOOL
CLINICAL PROGRAM IN CYBERLAW

Bruce P. Keller
Phillip R. Malone
Baker House
1587 Massachusetts Ave.
Cambridge, MA 02138
(617) 495-7547

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
ISSUE PRESENTED FOR REVIEW	1
INTEREST OF <i>AMICI</i>	2
SUMMARY OF ARGUMENT	5
ARGUMENT	8
I. The Seven-Day Warrant Return Limit Should Not Apply to the Review and Analysis of the Contents of Computers Properly Seized Within Seven Days	8
A. Probable Cause, the Touchstone of the Search Warrant Requirement, Requires Only the Timely Execution of Warrants . . .	8
B. Post-Search Examination of Seized Computers Does Not Implicate Probable Cause Concerns	13
C. Concerns About Possible Degradation or Alteration of Data After a Computer Has Been Seized Are Minimal and Do Not Raise Probable Cause Issues	20
II. Limiting the Review of Computer Content to Seven Days or Less Would Severely Hamper Law Enforcement’s Ability to Conduct a Careful, Thorough and Responsible Forensic Analysis . .	25
III. General Standards of Reasonableness Already Adequately Protect The Timing and Conduct of Post-Seizure Analysis of the Contents of Computers	45
CONCLUSION	49

TABLE OF AUTHORITIES

CASES

Andresen v. State, 24 Md. App. 128 (1975),
aff'd sub nom. *Andresen v. Maryland*,
427 U.S. 463 (1976) 17

Commonwealth v. Atchue, 393 Mass. 343 (1984) 9

Commonwealth v. Aviles, 58 Mass. App. Ct. 459
(2003) 18

Commonwealth v. Blye, 5 Mass. App. Ct. 817 (1977) . 10

Commonwealth v. Cinelli, 389 Mass. 197 (1983),
cert. denied, 464 U.S. 860 (1983) 9

Commonwealth v. Cromer, 365 Mass. 519
(1974) 10, 11, 14, 15

Commonwealth v. Donahue, 430 Mass. 710 (2000) 9

Commonwealth v. Gonsalves, 429 Mass. 658
(Mass. 1999) 46

Commonwealth v. Fleurant, 2 Mass. App. Ct. 250
(1974) 10

Commonwealth v. James, 424 Mass. 770 (1997) 12

Commonwealth v. Malone, 24 Mass. App. Ct. 70
(1987) 10

Commonwealth v. Martino, 412 Mass. 267 (1992) . 18, 19

Commonwealth v. Matias, 440 Mass. 787 (2004) 12

Commonwealth v. Robles, 423 Mass. 62 (1996) 18

Commonwealth v. Scanlon, 9 Mass. App. Ct. 173
(1980) 10

Commonwealth v. Slome, 321 Mass. 713 (1947) 10

Morrison v. Selectmen of Town of Weymouth,
279 Mass. 486 (Mass. 1932) 7

<i>State v. Petrone</i> , 468 N.W.2d 676 (Wis. 1991) . . .	19
<i>State v. Valenzuela</i> , 130 N.H. 175 (1987)	12
<i>State v. VanLaarhoven</i> , 637 N.W.2d 411 (Wis.App. 2001)	19
<i>State v. Zinck</i> , 2005 WL 551447 (N.H. Sup. Ct. Feb. 4, 2005)	48, 49
<i>United States v. Brunette</i> , 76 F.Supp.2d 30 (D. Me. 1999)	48, 49
<i>United States v. Habershaw</i> , 2001 WL 1867803 (D. Mass May 13, 2001)	16
<i>United States v. Hargus</i> , 128 F.3d 1358 (10th Cir. 1997)	47
<i>United States v. Hernandez</i> , 183 F.Supp.2d 468 (D.P.R. 2002)	15
<i>United States v. Hill</i> , 322 F.Supp.2d 1081 (C.D. Cal. 2004)	22, 23, 29, 30, 42, 43, 47
<i>United States v. Hunter</i> , 13 F.Supp.2d 574 (D. Vt. 1998)	30
<i>United States v. Marin-Buitrago</i> , 734 F.2d 889 (2d Cir. 1984)	13, 47
<i>United States v. Mendel</i> , 746 F.2d 155 (2nd Cir. 1984)	23
<i>United States v. Santarelli</i> , 778 F.2d 609 (11th Cir. 1985)	47
<i>United States v. Syphers</i> , 296 F.Supp.2d 50 (D.N.H. 2003), <i>aff'd</i> 2005 U.S. App. LEXIS 22527 (1st Cir. Oct. 20, 2005).	16, 20, 21, 46, 47
<i>United States v. Syphers</i> , 2005 U.S. App. LEXIS 22527 (1st Cir. Oct. 20, 2005).	13, 16, 28, 46, 47
<i>United States v. Triumph Capital Group</i> , 211 F.R.D. 31 (D. Conn. 2002)	<i>passim</i>

<i>United States v. Upham</i> , 168 F.3d 532 (1st Cir. 1999)	19, 28, 35
<i>United States v. Zink</i> , 612 F.2d 511 (10th Cir. 1980)	23

CONSTITUTIONAL PROVISIONS, STATUTES AND RULES

Mass. Const. art. 14	8, 46
U.S. Const. amend. IV	8, 9, 46
G.L. c. 276, §1	9
G.L. c. 276, §2A	10
G.L. c. 276, §3A	1, 5, 10, 13
Fed. R. Crim. P. 41	13, 15

TREATISES

Michael R. Arkfeld, <i>Electronic Discovery and Evidence</i> (2003)	24
Eoghan Casey, <i>Digital Evidence and Computer Crime</i> (2d ed. 2004).	29, 35, 38, 41, 42, 44
W. LaFave, <i>Search and Seizure</i>	12
Brian L. Porto, <i>Timeliness of Execution of Search Warrant</i> , 2002 A.L.R.5th 20	12
Hon. J.A. Grasso, Jr. & Hon. C.M. McEvoy, <i>Suppression Matters Under Massachusetts Law</i> § 8-2 2003)	10, 19

OTHER MATERIALS

Carnegie Mellon Media Relations Press Release, *Carnegie Mellon University Researchers Develop New Sensor To Detect Computer Hard Drive Failures* (March 1, 2004), at http://www.cmu.edu/PR/releases04/040301_hdfailures.html 26, 27

J. Philip Craiger, Jeff Swauger & Chris Marberry, *Digital evidence obfuscation: recovery techniques* (2005), at <http://ncfs.ucf.edu/craiger.5778-85.SPIE.pdf>, to appear in *Proceedings of the Society for Optical Engineering Conference, Orlando, FL* 33

Dorothy E. Denning & William E. Baugh, Jr., *Hiding Crimes in Cyberspace* (1999), at <http://cryptome.org/hiding-db.html>, reprinted in B.D Loader & D. Thomas, eds., *Cybercrime* (1999) 33

Guidance Software, *EnCase Legal Journal* (June 2001), at <http://www.cosgroveconsult.com/documents/EnCase%20Legal%20Journal.pdf> 24

Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment, Institute for Security Technology Studies at Dartmouth College, at http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf (June 2002) 21

How Much Information? 2003, University of California, Berkeley School of Information Management and Systems (2003), at <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/> 26

Gary Kessler, *Steganography: Implications for the Prosecutor and Computer Forensics Examiner*, Child Sexual Exploitation Program Update, Volume 1, Number 1 (Summer 2004), at http://www.ndaa-apri.org/publications/newsletters/child_sexual_exploitation_update_volume_1_number_1_2004.html . . . 35

New Jersey Department of Law & Public Safety,
Division of Criminal Justice, *Computer Evidence
Search & Seizure Manual 22* (2000), at
<http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf> . . . 41

Michael G. Noblett, Mark M. Pollitt, and Lawrence
A. Presley, *Recovering and Examining Computer
Forensic Evidence*, Forensic Science
Communications, Volume 2,
Number 4 (October 2000). 27, 39

U.S. Dept. of Justice, Computer Crime and
Intellectual Property Section, Criminal Division,
*Searching and Seizing Computers and Obtaining
Electronic Evidence in Criminal Investigations* §
D.2 (2002), at
<http://www.cybercrime.gov/s&smanual2002.htm> . . . 17, 27

U.S. Dept. of Justice, Office of Justice
Programs, National Institute of Justice, *Forensic
Examination of Digital Evidence: A Guide for Law
Enforcement* (April 2004), at
[http://www.ncjrs.org/pdffiles1/
nij/199408.pdf](http://www.ncjrs.org/pdffiles1/nij/199408.pdf) 40, 41, 42, 44

Alec Yasinsac and Yanet Manzano, *Policies to
Enhance Computer and Network Forensics*,
Proceedings of the 2001 IEEE Workshop on
Information Assurance and Security 2001), at
<http://www.cs.fsu.edu/~yasinsac/Papers/MY01.pdf> . . . 35

COMMONWEALTH OF MASSACHUSETTS

APPEALS COURT

Worcester County

No. 2005-P-0375

COMMONWEALTH OF MASSACHUSETTS,
Appellee,

v.

MICHAEL E. BRYANT,
Appellant

On Appeal from Judgments of the Superior Court

BRIEF OF *AMICI CURIAE*
NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN AND
AMERICAN PROSECUTORS RESEARCH INSTITUTE
IN SUPPORT OF APPELLEE

ISSUE PRESENTED FOR REVIEW

Should the application of Massachusetts General Law, Chapter 276, § 3A, which requires search warrants to be executed and returned within seven days of issuance, be expanded to also require that the complex and time-consuming forensic review and analysis of the contents of a computer seized pursuant to a warrant be completed within the same seven-day period?

INTEREST OF AMICI¹

The National Center for Missing and Exploited Children ("NCMEC") is a non-profit organization founded in 1984. Operating in partnership with the Office of Juvenile Justice and Delinquency Prevention at the United States Department of Justice ("OJJDP"), NCMEC is devoted to preventing child abduction, locating missing children and assisting families that have suffered through such an experience. NCMEC also focuses on combating child exploitation, an increasingly difficult task given that the growth of the Internet has made it exponentially easier to distribute child pornography and otherwise victimize children. NCMEC sponsors initiatives such as the CyberTipline, through which citizens can report apparent child pornography and efforts to solicit children. It also assists with Internet Crimes Against Children ("ICAC") training, offered by OJJDP and designed to provide law enforcement agencies with resources to improve their ability to fight online threats to children.

¹Pursuant to Massachusetts Rule of Appellate Procedure 17, *amici* file this brief conditionally along with their Motion for Leave to File Brief *Amici Curiae*.

As a result, NCMEC has a unique perspective on the extent to which criminals use computers and related technology to create and traffic in child pornography and engage in other forms of insidious child exploitation. This viewpoint includes expertise in the increasingly sophisticated techniques available to criminals to hide or obscure incriminating evidence on computers, and in the resulting increase in the time, resources and diligence required for forensic specialists to locate, recover, decrypt, identify and analyze the files containing such evidence.

As *amicus*, NCMEC can provide this Court with valuable background on relevant practical and technical characteristics of computers and other electronic media and on the impact of such characteristics on the post-seizure analysis and review of the contents of computers.

The American Prosecutors Research Institute ("APRI"), founded in 1984 by the National District Attorneys Association ("NDAA"),² is a non-profit research resource and clearinghouse for prosecutors at all levels of government. Its multi-disciplinary staff

²The NDAA represents over 30,000 local prosecutors in 2,700 jurisdictions across America, who prosecute more than 95% of the nation's criminal cases.

of veteran researchers and prosecutors offers comprehensive, accurate, and practical resources such as background information, training, expertise on technology applications, access to experts and presenters, and assistance with policy development.

In 1985, Congress, through the Victims of Child Abuse Act, appropriated funding for APRI's National Center for Prosecution of Child Abuse ("NCPCA"). NCPCA has served child abuse prosecutors and other allied professionals for over twenty years in assisting these professionals in protecting children. Recognized as the preeminent trainer in child abuse prosecutions, NCPCA serves child abuse professionals through extensive research, training, publications and technical assistance on all areas of child abuse.

As computers have been used increasingly as both a means and an end in crimes against children, NCPCA has developed its Child Sexual Exploitation program to respond to this ever growing threat. In addition to national training and publications in this area, NCPCA operates as a clearinghouse for information on the investigation and prosecution of child sexual exploitation offenses. APRI's and NCPCA's extensive research and practical expertise in computer

forensics, along with their emphasis on developing practices and training for law enforcement, provide a valuable technical and practical perspective to assist the Court's resolution of the issues in this appeal.³

SUMMARY OF ARGUMENT

I. The seven-day search warrant return requirement of Massachusetts General Law, Chapter 276, § 3A ("Section 3A") is imposed as a result of concerns that the probable cause for having issued the warrant might become stale should the warrant's execution be delayed. For that reason, Section 3A is properly read as requiring that the warrant be **executed** at the location specified in the warrant within seven days. Section 3A should not be divorced from its intended and logical context and expanded to impose the additional and often impossible requirement that the **review and analysis** of the contents of the files stored on a computer (or other evidence, for that matter) obtained pursuant to a properly issued warrant must be **completed** within seven days. Post-seizure analysis does not raise probable cause staleness

³Amici wish to acknowledge the invaluable assistance of Harvard Law School and Berkman Center Clinical Program in Cyberlaw students Melinda Gordon and Rita Lomio in the preparation of this brief.

concerns because, once a warrant is executed, the probable cause that existed at that time is and remains essentially frozen. Put another way, at the moment a computer is seized whatever probable cause existed at that moment is fixed and does not change.

[Pages 8-13]

Other courts considering similar warrant-return time limits have consistently adopted the common-sense position that return deadlines cannot and should not be extended to the post-seizure analysis and review of the data contained on a computer. In fact, courts in Massachusetts and elsewhere routinely reject analogous attempts to truncate the post-seizure review and forensic analysis of non-computer evidence, such as review of voluminous documents, DNA testing, and chemical and firearms analysis. Any concerns regarding possible degradation or alteration of evidence stored electronically during a prolonged period of storage and analysis affect, at most, the ultimate probative value of such evidence, but are unrelated to the probable cause question. Such concerns are capable of being addressed through other means that simply do not implicate the seven-day return limit. [Pages 13-25]

II. Transforming the seven day limitation to force investigators also to review and analyze the contents of computers and other electronic storage devices would create tremendous impediments to the proper conduct of investigations. Computers store increasingly vast amounts of data, in an ever-growing number of file formats, and offer criminals numerous opportunities to hide, disguise, encrypt, delete and otherwise shield from discovery evidence and electronic contraband. These developments present daunting challenges to investigators who must carefully and painstakingly uncover and analyze the contents of seized computers. Completing this complex task in the seven days or less that follow the issuance and execution of a warrant would be difficult and often impossible. It is a canon of statutory construction to avoid such senseless interpretations.⁴

[Pages 25-40]

⁴See, e.g., *Commonwealth v. Slome*, 321 Mass. 713, 716 (1947) ("Every statute, if possible, is to be construed in accordance with sound judgment and common sense, so as to make it an effectual piece of legislation."), citing *Morrison v. Selectmen of Town of Weymouth*, 279 Mass. 486, 492 (1932).

Moreover, even in cases where the forensic analysis possibly could be conducted in some fashion in seven days, requiring such haste would increase the otherwise avoidable risks of errors, incomplete or sloppy review and intrusiveness. [Pages 40-45]

III. The havoc wreaked by expanding the seven-day requirement to apply to the analysis of a computer's contents would not be offset by any increases in privacy rights or legitimate limits on government discretion. Article 14 of the Declaration of Rights of the Constitution of the Commonwealth and the Fourth Amendment of the U.S. Constitution already impose a general reasonableness standard that has been applied as, and remains, an important and sufficient safeguard against police malfeasance or abuse of the warrant process in appropriate cases. [Pages 45-50]

ARGUMENT

- I. The Seven-Day Warrant Return Limit Should Not Apply to the Review and Analysis of the Contents of Computers Properly Seized Within Seven Days**
 - A. Probable Cause, the Touchstone of the Search Warrant Requirement, Requires Only the Timely Execution of Warrants**

Under Massachusetts law, no search warrant may issue without probable cause. See Mass. Const. art. 14;

Mass. Gen. Laws Ann. ch. 276, § 1 ("Section 1").⁵ To establish probable cause for a search warrant, an affidavit must contain "enough information for an issuing magistrate" to determine (1) that "the items sought are related to the criminal activity under investigation," and (2) that those items "reasonably may be expected to be located in the place to be searched at the time the search warrant issues." *Commonwealth v. Donahue*, 430 Mass. 710, 711-12 (2000) (quoting *Commonwealth v. Cinelli*, 389 Mass. 197, 213 (1983), *cert. denied*, 464 U.S. 860 (1983)) (emphasis added).

As a result, the first temporal limitation that justifies a warrant turns on whether the "'proof . . . of [the] facts [underlying the warrant application is] so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time.'" *Commonwealth v. Atchue*, 393 Mass. 343, 349 (1984) (quoting *Sgro v. United States*, 287 U.S. 206, 210 (1932)).⁶

⁵The requirement under the U.S. Constitution is the same. U.S. Const. amend. IV.

⁶The likelihood that the objects of the search will be found at the place to be searched, "depends on a number of factors, including the nature of the

Once a search warrant is issued under Section 1, a second temporal limitation becomes operative. The language of Massachusetts General Law, Chapter 276, § 3A requires a police officer to return the search warrant "as soon as it has been served and in any event not later than seven days from the date of issuance"⁷ Section 3A, in conjunction with the "immediate search" requirement of Massachusetts General Laws, Chapter 276, § 2A,⁸ imposes the requirement that a

property to be seized, the nature of the criminal activity involved, and the nature of the premises to be searched." Hon. J.A. Grasso, Jr. & Hon. C.M. McEvoy, *Suppression Matters Under Massachusetts Law* § 8-2, at I-8 (2003) (citing *Commonwealth v. Blye*, 5 Mass. App. Ct. 817, 818 (1977); *Commonwealth v. Scanlon*, 9 Mass. App. Ct. 173, 180-81 (1980); *Commonwealth v. Malone*, 24 Mass. App. Ct. 70 (1987); *Commonwealth v. Fleurant*, 2 Mass. App. Ct. 250 (1974)).

⁷The procedure of returning the actual paper of the search warrant, together with an inventory of items seized, has been deemed by the SJC to be a purely ministerial requirement. See *Commonwealth v. Cromer*, 365 Mass. 519, 521 n.3 (1974). Failure to physically return the search warrant will not render an otherwise legal search invalid. *Id.*

⁸Section 2A specifies the following language to be included in a search warrant:

We therefore command you in the daytime (or at any time of the day or night) to make an *immediate search* of (identify premises) (occupied by A.B.) and (of the person of A.B.) and of any person present who may be found to have such property in his possession or under his control or to whom

search warrant be *executed* within a "reasonable time," normally (except for certain limited exceptions) not to exceed seven days after issuance. *Commonwealth v. Cromer*, 365 Mass. 519, 525-26 (1974). After seven days, the search cannot be properly executed. *Id.*

The purpose behind both time constraints is to combat staleness concerns. In general, "[t]he longer the police wait before executing the warrant . . . the more likely it is that the situation will change so that the facts which supported the magistrate's determination of probable cause will no longer exist." *Cromer*, 365 Mass. at 524. It is precisely because "[a] warrant is issued upon allegation of presently existing facts," that police must conduct searches within a "reasonable" time. *Id.* at 524-525 (internal citation omitted). Otherwise, the circumstances that supported the finding of probable cause may change and the probable cause will effectively become "stale," a danger that is "especially high when the object of the search is any easily moved substance, such as narcotics." *Id.* at 524. As a result, the evidence is less likely to be found in the place searched if

such property may have been delivered. . . .
Mass. Gen. Laws Ann. ch. 276, § 2A (emphasis added).

execution of the warrant is not timely. *Id.*⁹

In short, these time limitations are purely probable cause-based. Probable cause must exist to believe that, *when the warrant is executed*, specified items may reasonably be expected to be located *in the place to be searched*. See, e.g., *Commonwealth v. Matias*, 440 Mass. 787, 788-89 (2004) (informant's information was not stale as it showed defendant was involved in continuing drug activity); *Commonwealth v. James*, 424 Mass. 770, 777-78 (1997) (probable cause existed to support a search warrant authorizing search of defendant's residence for knives, sneakers, dark clothing and face masks because such items had continuing utility to defendant and it was reasonable to believe they would be kept at his residence); see also *State v. Valenzuela*, 130 N.H. 175, 192 (1987) ("Stale probable cause, so called, is probable cause

⁹See also, W. LAFAVE, SEARCH AND SEIZURE § 3.7; Brian L. Porto, *Timeliness of Execution of Search Warrant*, 2002. A.L.R.5th 20, *2 ("The purpose of requirements for the timely execution of search warrants is to insure that, when execution occurs, there is probable cause to believe that the items that the warrant seeks are in the place to be searched. . . . Probable cause ceases to exist when it is no longer reasonable to presume that items that were once located in a particular place are still there because the information that placed them in that location is old and has become unreliable.").

that would have justified a warrant at some earlier moment that has already passed by the time the warrant is sought.").¹⁰ No other purpose is served by the warrant-return time limit.¹¹

B. Post-Search Examination of Seized Computers Does Not Implicate Probable Cause Concerns

It is the relationship between valid probable cause and "stale" probable cause that highlights the critical distinction between (1) a search executed within the

¹⁰The parallel federal warrant-return requirement, Rule 41 of the Federal Rules of Criminal Procedure, contains a similar limit on the time for execution of a search warrant in the federal system. See Fed. R. Crim. P. 41(e)(2)(b) ("The warrant must command the officer to . . . execute the warrant within a specified time no longer than 10 days."). This requirement, like § 3A in Massachusetts, stems from concern about staleness and dissipation of probable cause. See, e.g., *United States v. Syphers*, 2005 U.S. App. LEXIS 22527, *22 (1st Cir. Oct. 20, 2005) ("The policy behind the ten-day limitation in Rule 41 is to prevent the execution of a stale warrant."); *United States v. Triumph Capital Group*, 211 F.R.D. 31, 66 (D. Conn. 2002) (same); *United States v. Marin-Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984) (The federal "limitations exist to ensure 'the speediest possible execution of search warrants,' and to lessen the possibility that the facts underlying the warrant may change.") (internal citation omitted).

¹¹To the extent extended analysis of a computer raises concerns about providing the computer's owner with access to his or her files during the review period, those concerns can easily be dealt with by making timely, identical copies of the computer's hard drive and returning a copy to the owner. See *infra* at 22-23 & n.15.

statutory period and (2) a post-seizure analysis of the items lawfully obtained during that search, whether the analysis consists of a review of the contents of a seized computer, examination of voluminous documents, or scientific or forensic testing such as blood, DNA or firearms analysis. In the latter context of post-seizure analysis, the probable cause that supported the warrant has effectively been "frozen" when the evidence is seized and will not change. In fact (assuming proper chain of custody and evidence-preservation protocols are followed), no staleness issues of any sort, even as to the probative value of the seized evidence, should arise.

This conclusion is entirely consistent with the Supreme Judicial Court's decision in *Cromer*. There, the court was confronted with and addressed only the *initial search of premises* for drugs and drug paraphernalia, the paradigmatic situation of "easily moved substance[s]," where the situation can change quickly and staleness issues can arise. 365 Mass. at 524. The court did not address the *post-seizure analysis* of such evidence (and of course not of computers or electronic materials), and *Cromer* certainly cannot be read as contradicting the common-

sense principle that staleness concerns no longer exist once evidence is seized. *See id.*

It is not surprising, therefore, that in the analogous context of Rule 41 of the Federal Rules of Criminal Procedure, courts uniformly have held that the contents of computers, once seized, may be reviewed and analyzed beyond the 10-day period because such analysis does not implicate any staleness concerns. For example, in *United States v. Triumph Capital Group*, 211 F.R.D. 31 (D.Conn. 2002), the court held that "neither Rule 41 nor the Fourth Amendment impose any time limitation on the government's forensic examination of the evidence seized," *id.* at 66, and rejected an argument that examination of seized computer data after the warrant return was filed was a post-search return "to a crime scene to search for additional evidence." *Id.* at 65. "[W]hen the mirror image [of the computer hard drive] was made within the ten-day period the evidence was frozen in time. Thus, there was no danger that probable cause ceased to exist during the search of the hard drive." *Id.* at 66. *See also United States v. Hernandez*, 183 F.Supp.2d 468, 480-81 (D.P.R. 2002) ("Neither Fed.R.Crim.P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer

may undergo a government forensic examination after it has been seized pursuant to a search warrant. . . . The examination of these items at a later date does not make the evidence suppressible.").

United States v. Habershaw, 2001 WL 1867803 (D. Mass. May 13, 2001), succinctly highlights the distinction between an initial search of premises supported by probable cause within the 10-day period and the subsequent post-seizure analysis of the items lawfully seized:

This execution of the warrant, namely the seizure of the electronic information on the hard drive, took place well within the ten days allowed. Further forensic analysis of the seized hard drive image does not constitute a second execution of the warrant or a failure to 'depart the premises' as defendant claims, any more than would a review of a file cabinet's worth of seized documents.

2001 WL 1867803 at *8 (emphasis added).

United States v. Syphers, 296 F.Supp.2d 50 (D.N.H. 2003), *aff'd* 2005 U.S. App. LEXIS 22527 (1st Cir. Oct. 20, 2005), in which the court rejected a challenge to a seven-month post-seizure inspection of a computer in a child pornography investigation, makes a similar point:

[J]ust as probable cause existed to support a search of the CPU when the warrant issued . . . , probable cause also existed to support the search at any time during the next year,

because the CPU was under the exclusive control of the police during that period.

296 F.Supp.2d at 58. See also *United States v. Gorrell*, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (upholding a 10-month delay and finding that "the warrant did not limit the amount of time in which the government was required to complete its off-site forensic analysis ... and the courts have not imposed such a prophylactic constraint on law enforcement."); *Andresen v. State*, 24 Md. App. 128, 172 (1975), *aff'd sub nom. Andresen v. Maryland*, 427 U.S. 463 (1976) (noting, in the context of extensive seizure of paper records and files, that "[i]n terms of nonstaleness, the probable cause here was still as the first dew of the morn"); U.S. Dept. of Justice, Computer Crime and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* § D.2 (2002) (the "government ordinarily may retain the seized computer and examine its contents in a careful and deliberate manner without legal restrictions, subject only to Rule 41(e)'s authorization that a 'person aggrieved' by the seizure of property may bring a motion for return of the

property.").

That probable cause staleness concerns do not arise in connection with post-seizure review of a computer's contents is further bolstered by the way post-seizure examination of videotapes and lengthy DNA or other scientific testing have been addressed. In such cases, where the underlying evidence is not immediately observable, just as digital evidence stored on computer hard drives and peripheral equipment is invisible to the naked eye without further analytical steps, courts consistently have allowed post-seizure, off-site review without requiring a second warrant or otherwise suggesting such review raises any probable cause issues. See, e.g., *Commonwealth v. Martino*, 412 Mass. 267, 277 (1992) (lawful seizure of a videotape permits viewing of its contents without the need to obtain an additional warrant); *Commonwealth v. Robles*, 423 Mass. 62, 65 n.8 (1996) (granting defendant's motion to suppress a coat seized upon arrest on lack of probable cause grounds, but rejecting, in dicta, the defendant's arguments that "the warrant . . . did not authorize chemical analysis of the coat"); *Commonwealth v. Aviles*, 58 Mass. App. Ct. 459, 464 (2003) (allowing DNA testing of a t-shirt, noting "the Supreme Judicial

Court has concluded that where the police have lawfully obtained evidence, it may be subject to scientific testing").¹²

¹²One treatise on Massachusetts law concludes from such cases that post-return examination or "processing" is reasonable:

Sometimes, it is not readily apparent whether the contents of the lawfully seized container include the object of the criminal activity that is sought. *Information on computer disks, film or videotape in a camera, or bore markings on a firearm, for example, may require an additional step to process as evidence. Usually, a second search warrant is not required to perform the additional step.*

Hon. J.A. Grasso, Jr. & Hon. C.M. McEvoy, *Suppression Matters Under Massachusetts Law* § 8-2, at I-8 (2003) (emphasis added) (citing *Martino*, 412 Mass. at 277). See also, *State v. Petrone*, 468 N.W.2d 676, 681 (Wis. 1991) (permitting development of undeveloped film seized pursuant to a warrant without requiring an additional warrant because "[a] search warrant does not limit officers to naked-eye inspections of objects lawfully seized in the execution of a warrant"); *State v. VanLaarhoven*, 637 N.W.2d 411, 417 (Wis.App. 2001) ("*Petrone* and *Snyder* teach that the examination of evidence seized pursuant to [a] warrant . . . is an essential part of the seizure and does not require a judicially authorized warrant. Both decisions refuse to permit a defendant to parse the lawful seizure of a blood sample into multiple components, each to be given independent significance for purposes of the warrant requirement."). *Petrone* has been cited approvingly (although briefly) in the First Circuit in *United States v. Upham*, 168 F.3d 532, 536 (1st Cir. 1999), to support the holding that

Cases involving viewing a seized videotape or conducting scientific and chemical testing are predicated on the same underlying principle that makes extended post-execution analysis of computer contents reasonable: The lack of any basis for concern that the initial probable cause that supported the search and seizure will change or become stale after the material or container to be analyzed has been lawfully obtained and maintained in police custody. The timely nexus between likely criminal activity and the place to be searched is established at the time the search warrant is issued, and post-seizure testing of lawfully seized and appropriately preserved items does not call into question that original probable cause determination.

C. Concerns About Possible Degradation or Alteration of Data After a Computer Has Been Seized Are Minimal and Do Not Raise Probable Cause Issues

As *Syphers* and the other cases cited above recognized, evidence stored on a computer remains static from the moment of acquisition, so once a computer is seized and its contents are under the exclusive control of the police, probable cause

"extraction of unlawful images from within the computer and diskettes was therefore contemplated by the warrant". *Id.*

remains the same as at the time of seizure. 296
F.Supp.2d at 58. Because of the physical
characteristics of computers, the risk of possible
degradation or alteration of the data on a computer
after it is seized is slight.¹³

In any event, concerns about the ultimate
integrity or probative value of the seized data do not
raise the issues of stale probable cause that underlie
the seven-day limit. Instead, such concerns raise
evidentiary issues regarding the reliability and
admissibility of evidence which are readily addressed
by a number of straightforward chain of custody and
evidence-preservation protocols. These protocols
drastically reduce any risk that seized electronic
materials might be altered, manipulated, or damaged in
the process of analysis.

First, forensic investigators typically begin

¹³Although some natural degradation of magnetic
computer data may occur over time, that will not
alter the *substance* of the data. See *Law Enforcement
Tools and Technologies for Investigating Cyber
Attacks: A National Needs Assessment*, Institute for
Security Technology Studies at Dartmouth College at
40-41 (June 2002) (examining an algorithm intended to
be used by law enforcement to ensure the integrity of
a seized storage device). In any event, the standard
forensic practice of making an identical duplicate
image of all the data immediately after seizure makes
this slight risk essentially irrelevant.

their analysis by making and preserving an identical copy of the original computer hard drive or other storage medium.¹⁴ All forensic examination and analysis can then be performed on the copy, rather than the original, thereby protecting the original hard drive from inadvertent alteration or manipulation. See *Triumph Capital*, 211 F.R.D. at 46 ("making a mirror image of the hard drive is . . . done to maintain the integrity and security of the original evidence"). Creating timely copies of the seized computer's contents also allows the authorities to provide the defense and its experts with an identical "image" of those contents. The defense then has a full opportunity to verify and duplicate the government's analysis and to confirm that the government's search did not alter or manipulate the evidence. See, e.g., *United States v. Hill*, 322 F.Supp.2d 1081, 1091-92 (C.D.Cal. 2004). In addition,

¹⁴An image copy (also sometimes known as a forensically-sound duplicate or "mirror image") of a hard drive is "an exact duplicate of the entire hard drive, and includes all the scattered clusters of the active and deleted files and the slack and free space." *Triumph Capital*, 211 F.R.D. at *48. The hard drive is the primary means of data storage on a computer. *Id.* at *45 n.4.

the copy permits the defendant to have access to and use of all of his or her files, programs and information while the forensic analysis is being conducted.¹⁵

Second, proper computer forensic protocols permit the government to establish that the electronic evidence it wishes to introduce in fact is "the seized object and that its condition is materially unchanged," *United States v. Zink*, 612 F.2d 511, 513 (10th Cir. 1980), typically by showing a solid chain of custody that "indirectly establishes the identity and integrity of the evidence by tracing its continuous whereabouts." *Id.* See also *United States v. Mendel*, 746 F.2d 155, 166 (2nd Cir. 1984). For example, the court in *Triumph Capital*, in upholding the reasonableness of the computer search and the

¹⁵Of course, the defendant himself (as distinguished from his counsel and expert) should still properly be denied access to any contents of his computer that are themselves contraband, such as images of child pornography, since the defendant's possession of those files is itself unlawful and results in an additional or ongoing victimization of the child victim. See, e.g., *Hill*, 322 F.Supp.2d at 1093 (imposing stringent limits on defense counsel and expert's handling of alleged child pornography and ordering that "defendant himself shall not be permitted to access or view any graphic image file containing actual or alleged child pornography . . . without petition and prior order of this Court.").

admissibility of the evidence gathered during it, relied in part on a showing that the investigator had maintained adequate records of his search and had documented his steps. 211 F.R.D. at 64.¹⁶ See also Michael R. Arkfeld, *Electronic Discovery and Evidence* 4-11 (2003) ("A forensic expert should be able to testify as to the chain of custody and help establish authenticity as needed.").

Simply put, extending the seven-day warrant-return limitation to the analysis of properly seized computer files would not assist a given criminal defendant's ability to raise doubts about how his or her computer files may have been treated post seizure. Instead,

¹⁶Certain types of commercial software products commonly used for forensic analysis often contain their own automatic chain of custody and documentation capabilities. See, e.g., Guidance Software, *EnCase Legal Journal*, p. 41 (June 2001):

[T]he EnCase process [has] documented chain of custody information that is automatically generated at the time of acquisition, and continually self-verified thereafter. The time and date of acquisition, the system clock readings of the examiner's computer, the acquisition MD5 hash value, the examiner's name and other information are stored in the header to the EnCase Evidence File. This important chain of custody information cannot be modified or altered within EnCase, and EnCase will automatically report a verification error if the Case Info File is tampered with or altered in any way.

the defendant remains free to do so in any number of ways. By contrast, as explained below, creating a new, seven-day limit on analysis would seriously hamstring essential forensic analysis and could, in many cases, result in sloppier, more-poorly documented or more intrusive review.

II. Limiting the Review of Computer Content to Seven Days Or Less Would Severely Hamper Law Enforcement's Ability to Conduct a Careful, Thorough and Responsible Forensic Analysis

As a practical matter, warrants often are not and cannot be safely and properly executed on the day they are issued. As a result, extending the seven-day warrant-return limit to the completion of all forensic analysis would often result in an even shorter period, at times as little as a couple of days, for that analysis. Forensic examination of data stored on a seized computer, however, is a complex, painstaking and time-consuming process that will continue to become even more so as storage capacity increases and computer technology expands. In many cases, a thorough review simply cannot, even today, be completed in seven days, let alone fewer, and this inability will only increase as computer storage becomes larger and more complex.

Even assuming an unlikely, full seven-day review period, however, and even in cases where some form of analysis might be capable of being conducted in that time period, the extreme deadline would force investigators to rush their analysis and would be likely to lead to an increased risk of incomplete or sloppy review, otherwise avoidable errors and increased intrusiveness. These harms would all be imposed without any increase in the prevention of stale probable cause or other corresponding benefit.

The serious disruption that would result from imposing a seven-day (or any similar fixed) limit for data analysis stems directly from the inherent technical characteristics of computers and the data stored on them.

1. Today, even a single computer can store a vast quantity of data, and multiple computers or a network of computers, including servers, contain drastically more.¹⁷ The United States Department of Justice

¹⁷Even standard personal computers today can easily contain tens of thousands or hundreds of thousands of separate files. Two years ago, most new personal computers *already* had a hard disk storage capacity in the range of 20 gigabytes. *How Much Information? 2003*, University of California, Berkeley School of Information Management and Systems (2003); that number has continued steadily to increase. One

("DOJ"), in its primary electronic search manual, concludes that, "Despite the best efforts of the government to analyze seized computer quickly, the forensic examination of seized computers often takes months to complete because computers can store enormous amounts of data." U.S. Dept. of Justice, Computer Crime and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* § D.2 (2002). Forensics experts support this conclusion, noting that, given the current capacities of computers, it is "impossible from a practical standpoint to completely and exhaustively examine every file stored on a seized computer system." Michael G. Noblett, Mark M. Pollitt, and Lawrence A. Presley, *Recovering and Examining Computer Forensic Evidence*, Forensic Science Communications, Volume 2, Number 4 (October 2000) ("Noblett Report").

Several courts have expressly acknowledged the impact that the large storage capacities of computers

gigabyte is equal to a "billion bytes - the equivalent of a billion English letters." Carnegie Mellon Media Relations Press Release, *Carnegie Mellon University Researchers Develop New Sensor To Detect Computer Hard Drive Failures* (March 1, 2004).

have on the amount of time needed to analyze them. See, e.g., *United States v. Syphers*, 2005 U.S. App. LEXIS 22527, *22 (1st Cir. Oct. 20, 2005)(upholding a seven-month analysis of computer data conducted after a five-month delay and noting that courts "have permitted some delay in the execution of search warrants involving computers because of the complexity of the search"); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (recognizing the consequences of expansive data storage capacity in a child pornography investigation and noting that "it is no easy task to search a well-laden hard drive"); *Triumph Capital*, 211 F.R.D at 66 ("computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution").¹⁸ For this reason, courts have upheld the reasonableness, and indeed the necessity, of post-seizure, off-site review of the contents of computers.

¹⁸The "magnitude of the information and data contained on [a] hard drive" would require a comprehensive (and presumably lengthy) review process). 211 F.R.D. at 61

2. It is well recognized that computer data is not only vast in quantity but also is stored in a large variety of formats and file types.¹⁹ "Unique file formats" now number in the "hundreds of thousands," thus demanding the use of a variety of time-consuming data review methods. Eoghan Casey, *Digital Evidence and Computer Crime* (2d ed. 2004) at 231. Moreover, the nature of computers and electronic data storage provide a myriad of ways in which users can hide, disguise or obscure their files:

'Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent.' . . . Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extension of files to disguise their contents to the casual observer. . . . *There is no way to know what is in a file without examining its contents, just as*

¹⁹File types are various storage formats utilized by computer programs. For example, documents are typically saved by word processing programs as some form of text files, photographs are typically saved as graphic files and songs or music are typically saved as audio files. File extensions are the specific labels or tags appended to the filename of individual pieces of content that conventionally indicate the file type. For example, 'TXT' and 'DOC' extensions are typically, though not always, associated with text or word processing files, 'JPG' and 'GIF' typically denote graphical images, and 'WAV' or 'MP3' typically indicate audio files.

there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised--whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated--forecloses defendant's proposed search methodology [based on file names or extensions].

United States v. Hill, 322 F. Supp. 2d 1081 1090-91 (C. D. Ca. 2004)(emphasis added) (quoting *United States v. Hunter*, 13 F.Supp.2d 574, 583 (D.Vt.1998)). See also *Triumph Capital*, 211 F.R.D. at 62 ("a computer user can mislabel or deliberately label files to avoid detection").

The ease with which criminals can manipulate file types and extensions to conceal damning electronic evidence, and the resulting need for thorough, time-consuming forensic analysis to locate such hidden evidence, is illustrated by *United States v. Harding*, 273 F. Supp. 2d 411 (S.D.N.Y. 2003), which concluded that it was not reasonable to require warrants to specify the particular file types sought:

[Although] file extensions 'generally' or conventionally indicate the nature of the content of the files to which they are assigned, that is not uniformly true. Files containing graphical images may be assigned file extensions, including 'TXT', that typically are assigned to text files. Files containing text may be assigned file extensions, including 'JPG' or 'GIF', that

typically are given to graphical image files. Hence, the agents who executed the warrant could not have determined simply from the file names and extensions that the files on the zip disk . . . contained the alleged child pornography . . . [rather than] other material. . . . *They could have done that only by opening and inspecting the contents of the files, without regard to the file extensions they bore . . .* Even if file extensions were unequivocally indicative of the nature of the files' contents . . . agents still would have had to open and inspect the [electronic] files in order to determine whether they contained evidence of the alleged fraud.

Id at 424 (emphasis added).

3. Forensic analysis of the contents of a computer is much more complex and sophisticated than merely determining whether files on the computer contain relevant evidence of a crime such as images of child pornography, emails exchanged with a minor, or fraudulent invoices. Rather, the analysis often will seek to reveal evidence by examining the overall context for the files; background information about their creation, storage and movement; and subtle and complex details about their interrelationship with other files or bits of evidence on the computer.

For example, in a child pornography investigation, a forensic analyst may need to look not only for illegal images themselves but also for evidence of

intent: *i.e.*, what search terms did the defendant use on the Internet, was he a member of known child-porn newsgroups, did he take steps to hide or disguise the images he downloaded, such as changing the names of the downloaded files or placing them in discrete folders, etc. The analyst also may try to identify the source of the images, perhaps determine if the defendant himself created or altered the images, or discover whether the images were further disseminated and to whom. Similarly, to establish a solid connection between the defendant and the illegal images, the analyst may need to examine other files to determine who was using the computer at the time the crime was committed; he might check to see whether an e-mail was sent or a diary entry was made within a short time of the images being downloaded or saved and, if so, by whom. The analyst also might work to evaluate a possible defense that the image may have been introduced onto the computer without the defendant's knowledge by a virus or other means. These are only a few examples of the extraordinary complexity presented by the examination of seized computers.

4. Criminals easily can restrict access to or encrypt the files on their computers. Encryption takes many forms, ranging from fairly simple password protection to extraordinarily sophisticated techniques utilizing advanced mathematical algorithms. See Dorothy E. Denning & William E. Baugh, Jr., *Hiding Crimes in Cyberspace* (1999), at <http://cryptome.org/hiding-db.html>, reprinted in B.D. Loader & D. Thomas, eds., *Cybercrime* (1999).

In the absence of the computer user's password or encryption key, the investigator must engage in "cracking" in an attempt to gain access to the protected files. *Id.* Password cracking is an "exhaustive time consuming approach." J. Philip Craiger, Jeff Swauger & Chris Marberry, *Digital evidence obfuscation: recovery techniques* §1.5.1 (2005); to appear in *Proceedings of the Society for Optical Engineering Conference, Orlando, FL* ("Craiger Report").²⁰

One variation of encryption, steganography, is a sophisticated technique that permits a computer user

²⁰In some cases, the need to use decryption techniques "delay[s] investigations, sometimes by months or years, and add[s] to their cost, . . . costing agencies hundreds of thousands of dollars to crack open encrypted files." Denning and Baugh.

to hide data (e.g. a text or spreadsheet-type business record containing evidence of fraud) invisibly within a media file, such as "an MP3 file or a graphical image." Craiger Report §2.2. Steganography allows individuals to embed data in an increasing range of file formats, including "executable files and spam messages." Gary Kessler, *Steganography: Implications for the Prosecutor and Computer Forensics Examiner*, Child Sexual Exploitation Program Update, Volume 1, Number 1 (Summer 2004). It poses particular challenges to computer forensic investigators because it "hides the very existence of a communications channel." *Id.* Identifying and decoding steganography can drastically slow the analysis of the contents of a computer that has been seized in a search.

5. Forensic analysis of the contents of computers frequently involves detecting and restoring files that the user took steps to delete but which still remain, invisible without careful analysis, on the hard drive.²¹ Locating and restoring "deleted" files is an

²¹At least on computers running the Windows operating system, "when a user deletes a file, the data in the file is not erased, but remains intact in the cluster or clusters where it was stored until the operating system places other data over it. . . . Unless there is sufficient data in a new document or file to

exacting and time-consuming task. See *Upham*, 168 F.3d at 535 (complex task to search a hard drive and other storage media "for information that may have been 'deleted.'"); Casey at 266 ("the recovery process is time-consuming"). Individuals who seek to prevent data recovery can greatly enhance the inherent difficulty of this effort by using "scrubbing tools and shredding software, which are programs designed to destroy information."²² Alec Yasinsac and Yanet Manzano, *Policies to Enhance Computer and Network Forensics*, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security at 293 (2001).

6. These and other daunting complexities in the forensic analysis of computer data cannot reliably be

overwrite all of the deleted data in the cluster, the cluster will contain remnants of formerly deleted data in the cluster's "slack space"--the space between the end of the new data and the end of the cluster. When all the clusters of a deleted file remain unused by the computer's operating system, it is possible to recover the deleted file in its entirety. Portions of deleted files may be recovered even if portions of the clusters the file occupied are being used by new files." *Triumph Capital*, 211 F.R.D. at 46, n. 8.

²²These programs "wipe clean the targeted space by writing over clusters several times. In some cases, even after the clusters are overwritten several times, the data or at least part of it can be recovered; however, the time spent in data recovery increases greatly." Casey at 266.

overcome in many cases by substituting automated review techniques for careful human forensic analysis. For example, keyword searches (see App. Br. at 23-24), typically involve using forensic software to scan the full text of the computer's text files for a variety of words that might be expected to be found in evidence of the sort specified by the warrant.²³ To be sure, keyword searching can be a useful and time-saving technique in certain circumstances, particularly when employed *in conjunction with* other techniques and an appropriate degree of careful human review. Keyword searching, however, like other automated review procedures, is not capable of fully solving the various technical problems just described.

Taking just the keyword review technology as an example, a few of its limitations demonstrate well why automated methods cannot be substituted completely for human review and judgment in many cases. Criminals easily can exploit the under-inclusive nature of keyword searches to hide evidence and evade seizure. Keyword searches, like other automated procedures,

²³For example, when searching for evidence of online child solicitation, investigators may use this method as one means of locating documents that contain words such as "sex," "travel" or "child" or the name of the victim or her hometown.

cannot in most cases recognize innuendo, unexpected slang or code words. Just as labels on either paper or digital documents can be disguised or coded, so can the actual words used in the body of digital documents. Criminals need not and ordinarily do not use predictable words such as "minor," "child pornography," "fraud," etc. As a result, they can readily mask a record or discussion of almost any subject and make it safe from keyword searching in all but the most unusual situations (e.g., where the police have an informant who can tell them every code word used by the suspects). See *United States v. Gurs*, 1996 U.S. App. Lexis 10976 at *8 (9th Cir. 1996) (where investigators sought electronic evidence of an illegal real estate scheme, the court determined that limiting the investigation to a keyword search would be unreasonably under-inclusive; "it was reasonable for the officers to look at files that were not 'flagged' through the 'key-word' system. Just because a file does not contain a particular word or combination of words does not mean that the document is outside the scope of a search.").

Compounding the problem, keyword searches are simultaneously over-inclusive and may identify

irrelevant documents that happen to contain the key term. Relying on keyword searches alone, without a degree of human judgment appropriate to the particular case, leads investigators to "miss important clues," while "floundering in a sea of superfluous data." Casey at 230.

More fundamentally, text documents such as emails, diary entries or spreadsheets can be made impervious to keyword searches or other text-based, automated methods by the simple process of converting them into image files through scanning or taking digital photographs. Such an image will be readable by sight in the same way as any text document, but cannot be searched electronically. See *Harding*, 273 F. Supp. 2d at 424. ("Text files containing such evidence are readily scanned and converted into graphical image files.") *Id.*²⁴ Thus, forcing investigators to use only

²⁴ With inexpensive scanners becoming pervasive, it is reasonable for investigators to expect that receipts, letters, emails, spreadsheets and any other documents may be stored not in text form but as images, and not with a 'TXT' or 'DOC' or 'XLS' extension but with a GIF or JPG or other "image" extension. Such scanning and file-type alteration may be done intentionally to hide or disguise incriminating materials, or for more innocent reasons: It is a growing practice for people to scan bills, other financial papers, letters and similar documents into their computers to create an image-file copy for their records. It is also

automated review techniques such as keywords, either directly or as a necessary tool to expedite computer searches to fit an artificial review deadline, in many cases would come at a high price in terms of missed evidence.

7. In certain cases, including that of Bryant in this appeal, investigators may have the added burden of assessing whether any of the computer files they review contain information subject to the attorney-client privilege (or other privileges such as the doctor-patient privilege) and, if so, ensuring that such information is not inadvertently disclosed to the team of lawyers and investigators responsible for prosecuting the defendant. See, e.g., *Triumph*, 211 F.R.D. at 42; Noblett Report (investigators must also take care to avoid "client and patient information that is privileged.").

These and other characteristics of computer data, and the difficulties they create for review once a

common for text documents to be emailed or otherwise sent to computers in a non-text format such as PDF or picture file. Whatever the motivation for their creation, the existence of such files requires forensic analysts to use comprehensive, multi-faceted analytical techniques and not rely exclusively on sometimes ill-fitting shortcuts such as keyword searches or file-type/extension searches.

search warrant is executed and a computer is seized, highlight the need for investigators to have adequate time and opportunity to utilize appropriate investigative techniques to ensure that all relevant information is detected and obtained in a manner that minimizes avoidable intrusion. Such forensic analysis demands flexibility, even if the most appropriate and effective process in a given case takes substantially longer than a quicker but more superficial or less comprehensive automated search method such as keyword searches. The reality is that no existing or anticipated technology or automated review method can replace the necessity for some degree of human analysis and judgment in the forensic examination process.

8. Finally, extending the seven-day limit for search warrant returns to the examination and analysis of seized computers and their contents would significantly increase, rather than decrease, concerns over maintaining the integrity of the seized data and minimizing the intrusiveness of the search.

First, computer data storage technology can be damaged or compromised if it is not handled in a careful, orderly way, typically in the controlled

conditions of an off-site forensics lab. See U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (April 2004) ("DOJ Guide") ("digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination."); Casey at 223 ("Any hardware and storage media collected must be preserved carefully. Preservation also includes a secure, anti-static environment such as a climate-controlled room.")

Moreover, in some circumstances, a computer user who wishes to ensure that certain files are not viewed by others can embed in the system destructive codes, sometimes known as "booby traps," that will cause the loss or overwriting of data if anyone tries to access the files without following precise procedures. See *Triumph*, 211 F.R.D. at 42.²⁵ Detecting and avoiding or

²⁵"Two common methods involve hot-keys and time-delay functions. A hot-key program destroys data, usually by overwriting or reformatting a disk, when a certain key is pressed. . . . A time-delay program monitors keyboard activity and starts to destroy data if no key is pressed within a certain period of time." New Jersey Department of Law & Public Safety, Division of Criminal Justice, *Computer Evidence Search & Seizure Manual* 22 (2000).

disabling booby traps requires a particularly careful, methodical examination in the controlled setting of a forensics lab.²⁶

Although routine, proper forensic protocols and procedures can minimize these and other risks of lost or damaged data, requiring investigators to complete complex analyses in a matter of a few days would have precisely the opposite effect. See *Hill*, 322 F.Supp.2d at 1088-89 (refusing to require the police to bring "equipment capable of reading computer storage media and an officer competent to operate it" to the premises because, among other problems, it would create "a serious risk that the police might damage the storage medium," which could then "compromise the integrity of the evidence." *Id.* at 1088-90); *Casey* at 108 ("Proper actions must be taken to ensure the integrity of potential evidence, physical and digital.")

Second, "in any thorough search for documents, even seemingly innocuous records must be examined to

²⁶In an Appendix containing sample affidavit language, the DOJ Guide specifies that, because data is subject to both "inadvertent or intentional modification or destruction . . . a controlled environment may be necessary to complete an accurate analysis." *DOJ Guide* Appendix F.

determine whether they fall with the category of items covered by the warrant." *Triumph Capital*, 211 F.R.D. at 63; *United States v. Hill*, 322 F. Supp. 2d at 1090-91 ("There is no way to know what is in a file without examining its contents"); *United States v. Harding*, 273 F. Supp. 2d at 424 (agents could determine if files contained "material relevant to the fraud allegations ... only by opening and inspecting the contents of the [computer] files.")

In many searches of computers, an assessment of the relevance of particular documents, images or other files ordinarily will require some degree of human judgment and involvement, even where other forensic techniques are utilized as well to help select or narrow the range of possible files. The more orderly and methodical the process of analysis, combining human review and automated techniques, the more likely it will be that investigators can carry out their legitimate evidence-gathering functions while also minimizing unnecessary intrusion. On the other hand, because of the often huge volume of files contained on computers and the time-consuming nature of conducting this human review properly, requiring investigators to rush their analysis likely would result in the

acquisition of a larger number of files of marginal or even questionable relevance than would otherwise occur. This inevitably will result in greater, otherwise avoidable, intrusions on privacy rather any reduction in such intrusions. Defendants' and suspects' legitimate interests will suffer, as will the public interest in the truth-seeking process and in reasonable and accurate discovery of evidence specified in valid search warrants.

Third, imposing an extremely short deadline on what would otherwise be a careful and orderly analysis by investigators almost certainly would reduce the quality of documentation, recordkeeping and oversight of that analysis. Plainly, it is "important to accurately record the steps taken during the digital evidence examination." *DOJ Guide* at 19. Under the DOJ Guidelines, analysts are urged to take a number of valuable but time-consuming precautions, such as recording comprehensive notes and "document[ing] irregularities encountered . . . changes made to the system . . . [and] information obtained at the scene." *Id*; see *Casey* at 217 ("Documentation is essential at all stages of handling and processing digital evidence."); *Triumph Capital*, 211 F.R.D. at 64 (court

relied in part on a showing that the investigator had maintained adequate records of his search and had documented his steps). Such documentation, where complete and accurate, provides a valuable check on wholly irrelevant or unwarranted police intrusions and provides the defense a full factual record on which to base any motions to suppress that might be appropriate in a given case. These interests would be harmed by extending the seven-day warrant-return rule to the completion of all computer forensic analysis.

Overall, requiring investigators to prioritize speed over all other concerns - including thoroughness, accuracy, data integrity, relevance, and privacy - will make forensic analysis a riskier and more intrusive process but will not yield any positive benefits.

III. General Standards of Reasonableness Already Adequately Protect The Timing and Conduct of Post-Seizure Analysis of the Contents of Computers

Limiting the review and analysis of seized computers to seven days from issuance of a warrant would neither meaningfully reduce law enforcement officials' discretion nor prevent unwarranted intrusions on defendant's legitimate privacy interests. The conduct of any such analysis already is subject to

review for general reasonableness under Article 14 of the Declaration of Rights of the Constitution of the Commonwealth and the U.S. Constitution's Fourth Amendment. Mass. Const. art. 14; U.S. Const. amend. IV.

The Supreme Judicial Court explicitly has indicated that the applicable standard under any Fourth Amendment analysis is one based on reasonableness. In *Commonwealth v. Gonsalves*, a drug trafficking case involving seizure of evidence at a traffic stop, the Court refused to impose a bright-line rule granting police permission to require passengers to step out of vehicles. The Court expressed its disfavor for such measures, stating that "bright-line rules . . . undermine the Fourth Amendment's underlying touchstone of reasonableness." 429 Mass. 658, 665 n.5 (1999).

In the federal Rule 41 context, courts have consistently applied a reasonableness analysis when rejecting the application of the ten-day return limit. *See, e.g., Triumph Capital*, 211 F.R.D. 31, 61, 66 (D. Conn. 2002) (the "relevant inquiry is whether the search and seizure was reasonable under the circumstances," and delay in computer forensic analysis "is not unreasonable unless . . . probable cause no longer exists"); *Syphers*, 2005 U.S. App. LEXIS 22527,

at *21-22 (finding that "'unreasonable delay that results in the lapse of probable cause will invalidate a warrant'," but that delay alone "does not render inadmissible evidence seized") (quoting *United States v. Marin-Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984); *Hill*, 322 F.Supp.2d at 1088-89 (upholding, in child pornography investigation, the off-site review of seized computer storage media as reasonable under the circumstances).²⁷ Courts have been particularly sensitive to the impact of computer data capacity and characteristics on the assessment of reasonableness. See, e.g., *Syphers*, 296 F.Supp.2d at 58 (seven-month period to complete data review was reasonable due to the enormous quantity of data involved and the fact that it was encrypted).

²⁷A similar reasonableness standard is applied in warrant cases outside the computer context. See, e.g., *United States v. Hargus*, 128 F.3d 1358, 1363 (10th Cir. 1997) ("Officers' conduct . . . is governed by the Fourth Amendment's mandate of reasonableness." Off-site search of business records (including two filing cabinets) in a money laundering investigation was reasonable in light of the "impracticability of on-site sorting" and the fact that "on-site sorting would be . . . unduly time-consuming.") *United States v. Santarelli*, 778 F.2d 609, 615 (11th Cir. 1985) ("the relevant inquiry" in any analysis of a search warrant is "whether the search and seizures were reasonable under all the circumstances").

This reasonableness standard provides ample protection against potential abuse. For example, in *United States v. Brunette*, 76 F.Supp.2d 30, 32-33 (D. Me. 1999), investigators seized the computer of a suspected child pornographer pursuant to a warrant which, by its explicit terms (and a subsequent extension), required the police to complete their analysis within sixty days. The police, however, **did not even begin** analyzing the computer until after the sixty-day period had lapsed. *Id.* at 42. Finding both this wholesale failure and the lack of any explanation for it to be unreasonable, the court granted the motion to suppress the computer evidence. *Id.*

Similarly, in *State v. Zinck*, 2005 WL 551447, *1 (N.H. Sup. Ct. Feb. 4, 2005), a New Hampshire superior court suppressed computer evidence in a child pornography case after finding unreasonable the actions of investigators who "failed to begin the search for approximately 18 months," but then, once started, completed it in "just two weeks." *Id.* at *4.

The reasonableness standard is a flexible one that examines the particular forensic analysis methods and the circumstances under which the investigator used them. A finding of reasonableness should not require,

for example, that authorities utilize the "best available" (App. Br. at 22), most "state-of-the-art" (*id.* at 24) or "industry standard" (*id.* at 24, n. 10) analytical technology or forensic investigative techniques. No authority is cited to support this novel proposition and it is not the law. Rather, reasonableness is a standard that is flexible and practical by design, thus allowing for consideration of both the realities of computer forensic examination and the specific circumstances of a given case.

The reasonableness requirement already effectively limits the government's discretion. It allows investigators sufficient time to complete their analysis under the particular circumstances of a given case, but does not sanction the wholesale neglect of the data review or, as in *Brunette* and *Zinck*, an unwarranted delay in even commencing that review.

CONCLUSION

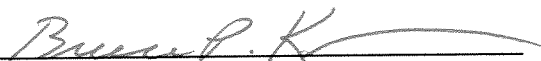
For the reasons set forth above, *amici* respectfully urge this Court not to take the unprecedented and extremely disruptive step of expanding the application of Section 3A's seven-day warrant-return rule to the forensic analysis of the contents of a properly seized computer.

CERTIFICATION

Pursuant to Rule 16(k) of the Massachusetts Rules of Appellate Procedure, counsel for amici certifies that this brief complies with the relevant rules that pertain to the filing of briefs, specifically Mass. R.App.P. Rules 16(b), 16(d), 16(g), 16(h), 16(k), 17, 19(a), 19(b) and 20, as applicable.

Respectfully submitted,

BERKMAN CENTER FOR
INTERNET AND SOCIETY
HARVARD LAW SCHOOL
CLINICAL PROGRAM IN CYBERLAW


Bruce P. Keller (BBO #264980)

Phillip R. Malone
Baker House
1587 Massachusetts Ave.
Cambridge, MA 02138
Telephone: (617) 495-7547

Dated: December 15, 2005