

NOTICE: All slip opinions and orders are subject to formal revision and are superseded by the advance sheets and bound volumes of the Official Reports. If you find a typographical error or other formal error, please notify the Reporter of Decisions, Supreme Judicial Court, John Adams Courthouse, 1 Pemberton Square, Suite 2500, Boston, MA 02108-1750; (617) 557-1030; SJCRreporter@sjc.state.ma.us

SJC-10177

COMMONWEALTH vs. HAROLD KAUPP.

Middlesex. November 3, 2008. - January 16, 2009.

Present: Marshall, C.J., Ireland, Spina, Cowin, Cordy, & Botsford, JJ.

Obscenity, Child pornography. Practice, Criminal, Motion to suppress. Probable Cause. Search and Seizure, Probable cause, Computer, Affidavit, Warrant. Constitutional Law, Search and seizure, Probable cause. Privacy.

Indictments found and returned in the Superior Court Department on November 11, 2002.

A pretrial motion to suppress evidence was heard by Regina L. Quinlan, J., and the cases were heard by Hiller B. Zobel, J.

The Supreme Judicial Court granted an application for direct appellate review.

Peter M. Onek, Committee for Public Counsel Services, for the defendant.

Casey E. Silvia, Assistant District Attorney, for the Commonwealth.

Dena T. Sacco for National Center for Missing and Exploited Children, amicus curiae, submitted a brief.

SPINA, J. The defendant was convicted of possession of child pornography in violation of G. L. c. 272, § 29C. On appeal he asserts error in the denial of his motion to suppress child pornography found on his computer because (1) the warrantless seizure of his computer was unlawful; (2) the affidavit in

support of the search warrant did not furnish probable cause to believe that his computer contained child pornography; and (3) the search of his computer over a period of months was unreasonable and in violation of G. L. c. 276, § 3A. We granted the defendant's application for direct appellate review. Because we conclude that the search warrant authorizing the search of the defendant's private files was not supported by probable cause that they contained child pornography, we vacate the order denying his motion to suppress and reverse the judgments of conviction.<sup>1,2</sup>

1. Warrantless seizure. We summarize the findings of the motion judge, supplemented by uncontested testimony from the motion hearing.

On May 21, 2002, James Smyth (James), a teacher and the technology director at the Northeast Metropolitan Vocational High School (high school) in Wakefield, was informed that an unauthorized computer named Joester7437 (Joester) was connected to the high school's network. James directed Holly Shepardson (Shepardson), a network specialist at the high school, to investigate Joester's contents and physical location on the high school's premises. From her computer, Shepardson accessed

---

<sup>1</sup> Given our conclusion that there was no probable cause to believe that the defendant had child pornography on his computer, we do not reach the defendant's claim that the colloquy regarding the waiver of his right to a jury trial was inadequate.

<sup>2</sup> We acknowledge the amicus brief submitted by the National Center for Missing and Exploited Children in support of the Commonwealth.

Joester's open share on the high school's network.<sup>3</sup> There, Shepardson found hacking tools, games, and pirated movies, and reported the same to James, prompting him to report the breach to a school administrator. Shepardson continued to examine Joester's open share and found a file titled "15 and 9 year old naked girls" that depicted pornographic images of two females, one of whom appeared to be in her late teens and another who appeared to be between nine and twelve years old. While James was apprising Vice Principal Theodore Nickole of the breach, Shepardson informed them of the pornography she had found in Joester's open share. James subsequently accessed Joester's open share and observed a pornographic image of a girl around ten years old. Officer Matthew Maglio, an officer assigned to the high school, also was present. After learning that child pornography had been found on Joester's open share, Officer Maglio contacted the Wakefield police department for assistance.

Shepardson then reported Joester's presence on the network to Timothy Smyth (Timothy), James's son and the high school's network manager. While trying to ascertain Joester's physical location within the high school, Timothy detected what appeared

---

<sup>3</sup> An open share facilitates the sharing of files among computers on a network by making certain resources on a computer available to other computers on the network. To create an open share, a computer user places the files to be shared in a folder and enables the sharing attributes of that folder to make that folder visible and accessible to other network users. An open share may be accessed by any user on the network, unless access is restricted to certain users.

to be five unauthorized computers on the school's network.<sup>4</sup> Within one hour, Timothy told James that he was "fairly certain" that the unauthorized computers were located in the electronics shop where the defendant was an instructor.

On the advice of James and before the police arrived, Vice Principals Nickole and Angela Antonelli went to the electronics shop, and asked the students and the defendant to go to the library. Sometime thereafter, Officer Maglio and Detective Lawrence James, a member of the Medford police department's computer crime unit, arrived at the electronics shop. Detective James spoke with James and Timothy as to what they had observed in Joester's open share. With the permission of Vice Principal Antonelli and James, Detective James, using his own notebook computer, accessed the school's network and opened Joester's open share. He found, inter alia, several movies, including "Spiderman." Detective James concluded that the copy of "Spiderman" was unauthorized as the movie had been released in theaters only recently. Detective James also found a motion picture file titled "Beautiful Lolita Sandra Masturbates" showing what appeared to be a young girl masturbating. With Timothy's assistance, Detective James subsequently located the Joester computer in the electronics shop and turned it off. The Joester computer, which was later determined to belong to a student, was seized and transported to the Wakefield police department.

---

<sup>4</sup> The school had generically denominated its computers. For example, a computer in the electronic shop might be named Electronics 1. The five unauthorized computers had unique names such as Joester7437 and Sinister.

While searching for unauthorized computers in the electronics shop, Timothy came across a school-owned server named Nightcrawler in the defendant's office, which was adjacent to the electronics shop.<sup>5</sup> Nightcrawler's screen displayed an open share containing the titles of several movies, including "Spiderman," "Top Gun," and "A Knight's Tale." The source of the open share was Sinister, another unauthorized computer logged onto the high school's network. Timothy did not see any pornographic materials in Sinister's open share. Sinister was also found in the defendant's office. However, Timothy could not log on to Sinister as it was password protected.

Detective James, having been apprised of Timothy's observations of pirated movies on Sinister's open share, seized Sinister, which belonged to the defendant, on probable cause to believe that it contained child pornography and copyrighted intellectual property. Detective James did not look at the contents of Sinister's open share prior to securing it.

In reviewing a motion to suppress, we accord substantial deference to the motion judge's subsidiary findings and will not disturb them absent clear error. Commonwealth v. Jones, 375 Mass. 349, 354 (1978). Our review of the application of constitutional principles to those facts, however, is plenary. Commonwealth v. Haas, 373 Mass. 545, 550 (1977), S.C., 398 Mass. 806 (1986).

---

<sup>5</sup> Timothy testified that a server is "the same as a desktop computer, other than the fact that its primary usage is to be used for others to remotely access it, to remotely use it to store files and things of that nature."

The defendant makes a number of arguments challenging whether Sinister was properly seized pursuant to an exception to the warrant requirement.<sup>6</sup> They lack merit. Timothy's observation of the then recently released movie "Spiderman" on Sinister's open share furnished probable cause to believe that Sinister contained pirated movies, prompting Detective James to impound Sinister. Detective James refrained from searching Sinister's contents until the search warrant issued. Cf. Commonwealth v. Gentile, 437 Mass. 569, 572-577 (2002) (seizure of defendant's clothing and truck prior to seeking search warrant was supported by probable cause and permissible where evidence would have likely dissipated had evidence not been seized). The impoundment of an object pending the issuance of a search warrant violates the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights only if it is unreasonable. See United States v. La France, 879 F.2d 1, 6 (1st Cir. 1989); Commonwealth v. Catanzaro, 441 Mass. 46, 55-56 (2004). See generally J.A. Grasso & C.M. McEvoy, *Suppression Matters Under Massachusetts Law* § 14-1[c][3][iv], at 14-8 -- 14-9 (2008-2009). Reasonableness necessarily turns on the facts of each case, requiring courts to "balanc[e] the need to search or seize against the invasion that the search or seizure entails." Commonwealth v. Catanzaro, supra at 56. Given the ease with

---

<sup>6</sup> We note that contrary to the defendant's understanding of the ruling below, the motion judge did not conclude that the school had consented to Sinister's seizure. Rather, she correctly ruled that the school consented to a search of its network, which included Sinister's open share. See Commonwealth v. Welch, 420 Mass. 646, 654 (1995); Commonwealth v. Wahlstrom, 375 Mass. 115, 117 (1978).

which computer files may be accessed and deleted, and the disruption that would have been created by posting an officer in the defendant's office and preventing students from entering pending the issuance of a search warrant, we conclude that the seizure was reasonable. See Commonwealth v. Hinds, 437 Mass. 54, 62 (2002), cert. denied, 537 U.S. 1205 (2003) (reasonable to seize computer because files easily could be destroyed and posting officer in home more intrusive than securing hard drive and keyboard).<sup>7</sup> Moreover, notwithstanding the defendant's contention to the contrary, the nine-day delay in seeking a search warrant did not render the seizure unreasonable. See United States v. Hall, 142 F.3d 988, 994-995 (7th Cir. 1998) (one-day delay in seeking search warrant for impounded computer

---

<sup>7</sup> The Commonwealth contends, and we agree, that the potential destruction or loss of evidence on Sinister created an exigency justifying the warrantless seizure of Sinister. See Illinois v. McArthur, 531 U.S. 326, 334 (2001) ("We have found no case in which this Court has held unlawful a temporary seizure that was supported by probable cause and was designed to prevent the loss of evidence while the police diligently obtained a warrant in a reasonable period of time"); Commonwealth v. Gentile, 437 Mass. 569, 572-577 (2002); Commonwealth v. Hinds, 437 Mass. 54, 62 (2002), cert. denied, 537 U.S. 1205 (2003). However, the Commonwealth maintains that the police did not need a warrant to search Sinister's contents because they seized Sinister pursuant to the exigent circumstances exception to the warrant requirement. We disagree. As we have noted, "an officer's authority to possess a package is distinct from his authority to examine its contents." Commonwealth v. Varney, 391 Mass. 34, 39 n.4 (1984), quoting Walter v. United States, 447 U.S. 649, 654 (1980) (opinion of Stevens, J.). The exigency necessitating Sinister's seizure dissipated once the computer had been secured, requiring the police to seek a search warrant to conduct a forensic analysis of Sinister's contents. See State v. Rupnick, 280 Kan. 720, 733 (2005) (appropriate to obtain warrant because exigency dissipated once computer seized). See also Commonwealth v. Straw, 422 Mass. 756, 759 (1996) (exigency to search briefcase expired once briefcase seized).

not unreasonable); People v. Shinohara, 375 Ill. App. 3d 85, 101 (2007) (two and one-half month delay in seeking search warrant for seized computer not unreasonable).

2. Probable cause. The defendant contends that Officer Maglio's affidavit did not establish probable cause to believe that there was child pornography on Sinister.<sup>8</sup> The defendant does not dispute that he did not have any reasonable expectation of privacy in the files in Sinister's open share, which were accessible to all network users. See United States v. King, 509 F.3d 1338, 1342 (11th Cir. 2007) (no reasonable expectation of privacy in files accessible to anyone on military base's network). Therefore, at issue is whether there was probable cause to search the defendant's private files, which were not available to other network users, for child pornography.

In reviewing a finding of probable cause, we consider only the facts recited in the affidavit and any reasonable inferences therefrom. Commonwealth v. Allen, 406 Mass. 575, 578 (1990). We summarize the facts recited in Officer Maglio's affidavit.<sup>9</sup>

The affidavit recounted how the presence of an unauthorized computer, Joester, on the high school's network was detected by high school personnel. On examination of Joester's open share, Shepardson discovered files containing child pornography, and files containing the movies "Spiderman" and "Star Wars, Episode

---

<sup>8</sup> The defendant does not challenge those portions of the search warrant pertaining to copyrighted intellectual property.

<sup>9</sup> The details of what was discovered have been described in the previous section. They were included in the affidavit and are intentionally not duplicated here.

II, Attack of the Clones," both of which were recently released in theaters.

Using an open network connection on Joester, Timothy accessed Nightcrawler, a "computer/server" on the network and reported observing another network computer that contained a list of file folders and directories "indicat[ing] 60-70 movie titles that were available for viewing on the computer named 'Sinister' . . . [Timothy] indicated three of these titles to be 'Top Gun,' a 'Knight's Tale,' and 'Spiderman.'" Based on his training and experience in computer investigations and computer networking, Officer Maglio stated that he reasonably believed that the "above mentioned electronic media files have been shared amongst the aforementioned computer systems through their existing shared resources and do reasonably believe that these files exist in electronic format on both of these computer systems." Sinister subsequently was located on the defendant's desk and seized "with the probable cause that it contained graphic child pornographic images, intellectual property and copy-written materials."

After Sinister's seizure, Officer Maglio and Detective Richard Cass interviewed the defendant.<sup>10</sup> The defendant acknowledged that he owned Sinister. He explained that he allowed students to place computer files in a folder titled "Drops" and that the students regularly left pornographic materials in the "Drops" folder. He admitted he had eighteen copyrighted movies and numerous computer viruses stored on

---

<sup>10</sup> The defendant received Miranda warnings prior to the interview.

Sinister.<sup>11</sup> He also admitted that he had a personal collection of pornography stored on his computer and that he often traded files containing pornographic images for software upgrades.<sup>12</sup> Officer Maglio stated that the defendant "could not guarantee that there were not any child pornographic images stored in electronic format within his computer."<sup>13</sup>

On May 30, 2002, Officer Maglio applied for a search warrant to search Sinister's hard drives and several electronic data storage devices found in Sinister. The affidavit in support of the search warrant stated that Officer Maglio had been a police officer for fifteen years, studied numerous software programs, hardware devices, books, articles, journals, and papers relating to computer security, computer crime, and high technology crime investigations, and received specialized computer crime investigation training. Officer Maglio indicated that some computer users encrypt, booby trap, hide, or otherwise conceal electronically stored data "in an attempt to hide their activities and prevent the collection of evidence against them." He also stated that persons with a demonstrated interest in child pornography were likely to retain such images for an extended

---

<sup>11</sup> The affidavit recounting the interview does not state whether the defendant had stored these items in his open share, his private files, or both.

<sup>12</sup> The affidavit did not state whether the defendant indicated that his pornography collection was in Sinister's open share, his private files, or both.

<sup>13</sup> Nothing in the affidavit indicates whether the defendant was referring to the files students placed in the "Drops" folder, other files in Sinister's open share, the defendant's private files, or his computer generally.

period of time and use multiple computers, electronic mail, and Internet accounts.

Based on the forgoing, the application requested permission to search Sinister's hard drives and the other electronic data storage devices for, inter alia, child pornography; any textual files referring to "past sexual acts and/or attempted sexual acts and/or solicitations involving the request for child pornography"; and copyrighted material. Citing the potential technical difficulties in recovering electronically stored data, Officer Maglio requested permission "to make exact duplicate copies of selected computer storage/media evidence for further forensic examination" and proposed to file an initial return of service within seven days, see G. L. c. 276, § 3A, and a supplemental return of service after the seven-day period.

An assistant clerk-magistrate in the Malden Division of the District Court Department issued the requested warrant, but did not address Officer Maglio's request for time beyond the seven-day period to file a supplemental return for purposes of completing a forensic analysis of the copies of Sinister's hard drives and assorted electronic data storage devices.

Detective James executed the search warrant by making a "mirror image" of Sinister's hard drives and the electronic data storage devices.<sup>14</sup> A return of service indicating which devices were copied was filed on June 6, 2002. By November, 2002,

---

<sup>14</sup> Neither party has made any distinction between Sinister's hard drives and the electronic data storage devices, mostly compact discs, found inside Sinister. For ease of reference, we refer to the hard drives and peripheral storage devices collectively as Sinister.

Detective James had conducted a forensic examination of the mirror images of Sinister's hard drives using EnCase software.<sup>15</sup> On Sinister's hard drives, he found a folder labeled "Joester transfers"<sup>16</sup>; pirated movies and software; hacking tools; and child pornography.<sup>17</sup>

A search warrant may issue only on a showing of probable cause. Commonwealth v. Byfield, 413 Mass. 426, 428 (1992). Under the Fourth Amendment and art. 14, probable cause requires a "substantial basis," Commonwealth v. Stewart, 358 Mass. 747, 749 (1971), for concluding that "the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues." Commonwealth v. Cinelli, 389 Mass. 197, 213, cert. denied, 464 U.S. 860 (1983). See

---

<sup>15</sup> At the time of the motion to suppress hearing in February, 2004, Detective James had not written a report of his forensic examination of Sinister. He explained, however, that EnCase software allowed him to "look at the file structures, files, folders, and information contained on the hard drive."

<sup>16</sup> In this file, Detective James found pirated movies and software, utilities to reverse engineer software, and adult pornography. He could not recall whether he found any child pornography. He confirmed that the files in "Joester transfers" were the same files as the files on Joester's open share by running a "hash," a complicated mathematical algorithm that produces similar output if files are identical and dissimilar output if they are not. See Howard, Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, 19 Berkeley Tech. L.J. 1227, 1233-1234 (2004).

<sup>17</sup> Detective James's testimony at the suppression hearing does not indicate whether the child pornography found on Sinister was found in Sinister's open share, the defendant's private files, or both. At trial, Detective James testified that he found the pornographic images giving rise to the indictments in the defendant's private files.

Commonwealth v. O'Day, 440 Mass. 296, 301 (2003); Commonwealth v. Upton, 394 Mass. 363, 370 (1985). "In dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Draper v. United States, 358 U.S. 307, 313 (1959), quoting Brinegar v. United States, 338 U.S. 160, 175 (1949). While an application for a search warrant need not make a showing beyond a reasonable doubt, Commonwealth v. Stewart, *supra*, "[s]trong reason to suspect is not adequate." Commonwealth v. Upton, *supra*.

In reviewing a finding of probable cause, the affidavit "should be interpreted 'in a commonsense and realistic fashion,' United States v. Ventresca, 380 U.S. 102, 108 (1965). See Commonwealth v. Burt, 393 Mass. 703, 714 (1985), and 'read as a whole, not parsed, severed, and subjected to hypercritical analysis.' Commonwealth v. Blake, 413 Mass. 823, 827 (1992)." Commonwealth v. Donahue, 430 Mass. 710, 712 (2000). An inference drawn from the affidavit, "if not forbidden by some rule of law, need only be reasonable and possible; it need not be necessary or inescapable." Commonwealth v. Beckett, 373 Mass. 329, 341 (1977).

After reviewing Officer Maglio's affidavit, we conclude that the affidavit, read as a whole and in a nontechnical manner, does not establish probable cause to believe that child pornography was located among the defendant's private files. The portions of the affidavit suggesting that the defendant's private files

contained child pornography consisted of (1) the fact that both Joester and Sinister had a copy of the recently released movie Spiderman, suggesting that the movie had passed from one computer to another; (2) the fact that child pornography had been observed in Joester's open share; and (3) Officer Maglio's statement that the defendant "could not guarantee that there were not any child pornographic images stored in electronic format within his computer." None of these facts, even when considered together, provided a "substantial basis" to believe that the defendant's private files contained child pornography.<sup>18</sup>

With respect to the presence of the Spiderman movie on both computers, the inference urged by the Commonwealth is simply too attenuated. The presence of Spiderman on both computers bears on probable cause only if it may reasonably be inferred that sharing an electronic copy of a commercial movie suggests an interest in sharing child pornography. Such an inference is not reasonable. The fact that the defendant could access child pornography does not advance the Commonwealth's contention that the defendant copied child pornography from Joester onto his computer. See United States v. Falso, 544 F.3d 110, 121 (2d Cir. 2008) (no probable cause where affidavit merely recited that defendant had ability to view child pornography on Web site defendant visited,

---

<sup>18</sup> We do not address whether the child pornography found in the defendant's private files would have been in plain view while searching those files for copyrighted material, see Commonwealth v. Hinds, 437 Mass. 54, 61 (2002) (child pornography in plain view during consented-to search for electronic mail relating to homicide), because the Commonwealth has not raised that issue and had the burden to do so. See Commonwealth v. Figueroa, 412 Mass. 745, 750 (1992); Commonwealth v. Bond, 375 Mass. 201, 210 (1978); Commonwealth v. Antobenedetto, 366 Mass. 51, 57 (1974).

but did not state whether defendant accessed, viewed, or downloaded child pornography). Moreover, although "the nexus between the items to be seized and the place to be searched need not be based on direct observation," Commonwealth v. Cinelli, supra at 213, nothing in the affidavit suggests that child pornography had been seen in Sinister's open share; and notwithstanding the defendant's poor judgment in failing to reprimand students for storing pornography in the "Drops" file on Sinister's open share, the affidavit does not indicate that students stored child pornography on Sinister, let alone that the defendant had transferred students' child pornography to his private files. The affidavit also does not suggest that the child pornography found in Joester's open share came from Sinister.

The Commonwealth urges us to draw an adverse inference from the defendant's admission that he had a personal collection of pornography on his computer. We decline to do so. The affidavit provides no basis to conclude that an interest in adult pornography (which, if not obscene, is constitutionally protected, see Miller v. California, 413 U.S. 15, 24-25 [1973]; Commonwealth v. Donahue, 358 Mass. 803 [1970]) is a basis to infer an interest in child pornography. See United States v. Falso, supra at 122 (rejecting inference between sexual abuse of minor and possession of child pornography where association was neither stated nor supported in affidavit).

The defendant's equivocal statement to Officer Maglio, although suspicious, also falls short of providing a "substantial

basis" for concluding that there was child pornography in the defendant's private files. Commonwealth v. Stewart, supra at 749. We have previously held that "[i]mplausible answers to police questions will, with other facts, support a finding of probable cause to conduct a search . . . as will peculiar behavior and evasive replies" (emphasis added). (Citations omitted.) Commonwealth v. Riggins, 366 Mass. 81, 88 (1974). See 2 W.R. LaFare, Search and Seizure § 3.6(f), at 360-362 (4th ed. 2004) (false, incriminating, implausible, conflicting, evasive, or unresponsive answers may constitute probable cause when considered with other factors). Such a statement standing alone, however, will seldom, if ever, provide a "substantial basis" for believing that the objects sought are probably present in the place to be searched. Commonwealth v. Stewart, supra. See United States v. Kelly, 547 F.2d 82, 84 (8th Cir. 1977) (doubting that single evasive answer concerning car's ownership sufficient to establish probable cause to believe car was stolen where police knew who owned car and that car had not been reported stolen); Jackson v. State, 745 S.W.2d 4, 9 (Tex. Crim. App. 1988) (declining to "sanction the notion that implausible, conflicting, evasive, or unresponsive answers to police queries by a criminal suspect alone constitutes probable cause"); Kraus v. State, 226 Wis. 383, 387-388 (1937) (statement "I don't know you, Mr., and furthermore I won't take a chance" in response to request for "a pint" insufficient to establish probable cause to believe that liquor was being unlawfully made, sold, possessed, or concealed). See also Commonwealth v. Alvarado, 420 Mass. 542, 549 (1995)

(furtive gesture, such as attempt to conceal object, does not by itself give rise to probable cause to seize object or for warrantless arrest). Thus, while it could reasonably be inferred that the defendant was intentionally ambiguous, such an inference, standing alone, does not provide a "substantial basis" for concluding that child pornography could be found on Sinister. We add that the defendant's ambivalence concerning the presence of child pornography on his computer stands in sharp relief to his candid admissions that he had eighteen copyrighted movies and various computer viruses stored on his computer.

We are mindful that investigations involving child pornography and computers are fraught with difficulty, requiring courts to balance the eminently desirable goal of eradicating child pornography on the one hand with an individual's privacy interests in the contents of a personal computer on the other. The probable cause standard and the forgiving eye with which courts read affidavits in support of search warrants provide law enforcement agents with sufficient leeway to demonstrate that the items sought are reasonably expected to be in the place to be searched. Nevertheless, the ability to access child pornography stored on Joester and the defendant's ambiguous statement did not constitute a "substantial basis" for concluding that the defendant stored child pornography in his private files. At best, the affidavit established a "[s]trong reason to suspect" that the defendant's private files contained child pornography. Commonwealth v. Upton, 394 Mass. 363, 370 (1985). This was insufficient.

3. General Laws c. 276, § 3A. The result we reach in this case makes it unnecessary to decide the question whether failure to complete forensic examination of the defendant's computer within seven days constitutes a violation of G. L. c. 276, § 3A, and requires suppression of the results of the search of his computer. However, where the question is one of public importance, is likely to arise again, and has been fully briefed, we exercise our discretion and consider the issue. See Allen v. Boston Redevelopment Auth., 450 Mass. 242, 254 n.20 (2007), citing Lockhart v. Attorney Gen., 390 Mass. 780, 783 (1984).

General Laws c. 276, § 3A, provides:

"Every officer to whom a warrant to search is issued shall return the same to the court by which it was issued as soon as it has been served and in any event not later than seven days from the date of issuance thereof, with a return of his doings thereon; provided, however, that a justice of the superior court may at any time receive complaints and issue search warrants returnable in seven days before a district court named in such warrant and in that event the officer shall make his return to such district court as directed."

The "required warrant return procedures are ministerial, and failure to comply therewith is not ground for voiding an otherwise valid search." Commonwealth v. Cromer, 365 Mass. 519, 521 n.3 (1974). In this case, the critical question is whether the search warrant was executed within seven days of its issuance. See id. at 524. Under similar provisions and rules in other jurisdictions, courts have held that the police do not need to complete forensic analysis of a seized computer and other electronic data storage devices within the prescribed period for executing a search warrant. See United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005), cert. denied, 547 U.S. 1158

(2006); United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002); State v. Grenning, 142 Wash. App. 518, 532 (2008). Because a written return listing the devices to be examined was filed seven days after the search warrant issued, there was no violation of G. L. c. 276, § 3A.

4. Conclusion. The order denying the defendant's motion to suppress is hereby vacated and the judgments of conviction are reversed.

So ordered.