Touro Law Review

Volume 30
Number 4 *Annual New York State Constitutional Issue*

Article 10

November 2014

Seize First, Search Later: The Hunt for Digital Evidence

Paige Bartholomew

Seize First, Search Later: The Hunt for Digital Evidence

Cover Page Footnote

30-4

SEIZE FIRST, SEARCH LATER: THE HUNT FOR DIGITAL EVIDENCE

COURT OF APPEALS OF NEW YORK

People v. DeProspero[1]
(decided March 26, 2013)

I. INTRODUCTION

The use of computers in criminal activity has popularized a new form of evidence known as digital evidence. Police officers and law enforcement agents now commonly seize and search computers in connection with criminal investigations, the evidence obtained from which is often critical to securing convictions. Computer searches, however, are much different from ordinary searches for physical evidence due to the complexity of information stored within a computer or hard drive as well as the technical expertise required to retrieve such evidence. Often times, the police seize a suspect's computer and take it to a police laboratory for extensive examination by forensics experts. These forensic examinations may take days, months, or even years.[2]

Currently, there are no bright line rules governing the scope of the police search or the amount of time law enforcement may ordinarily retain the seized property before returning it to a suspect. Not surprisingly, there have been many challenges to the constitutionality of computer searches, especially in the context of child pornography—in which the evidence found on a suspect's computer can be highly incriminating. Courts have grappled with these challenges and have attempted to apply constitutional restraints to ensure that the scope and execution of these searches fall within the limits prescribed by the

[1] 987 N.E.2d 264 (N.Y. 2013).

[2] *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV 279, 300-01 (2005) (emphasis added) (explaining the need for current laws to be amended so as to strike the proper balance between law enforcement needs and individual rights in property and privacy in light of existing technological realities).

Fourth Amendment.[3]

Despite varying approaches to this issue, courts and legislatures need not create new rules to address these concerns. Rather, existing Fourth Amendment principles can be applied in the context of computer forensic searches. These principles appropriately balance an individual's privacy interests with the state's interest in conducting a thorough search of digital evidence to protect society from sexual predators. The goal, then, is to strike a fair balance between the state's interest in protecting society from sexual predators and the privacy concerns that are part and parcel of the Fourth Amendment. If effective law enforcement requires forensic computer searches, then these searches should be permitted. However, investigators should begin the forensic analysis expeditiously and return any property that does not contain incriminating evidence "within a *reasonable* period of time."[4] Because the facts and circumstances differ in each case, what is considered reasonable in one situation may not be considered reasonable in another. Therefore, the reasonableness of an electronic forensics search should be determined on a case-by-case basis.

This case note will discuss the issue presented to the New York State Court of Appeals in *People v. DeProspero*—whether a subsequent forensic analysis of the defendant's computer, performed approximately seven months after the computer was initially seized and after the defendant had already served a prison sentence on related charges, violated the Fourth Amendment.[5]

II. *PEOPLE V. DEPROSPERO*

A. Factual & Procedural Background

In 2008 and 2009, an undercover New York State Police detective investigated individuals sharing child pornography on the Internet

---

[3] U.S. CONST. amend. IV:

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

Id.

[4] Kerr, *supra* note 2, at 313 (emphasis added).

[5] *DeProspero*, 987 N.E.2d at 265-66.

through various file-sharing networks.[6] A particular IP address was suspected of downloading child pornography files over forty times between February and March of 2009.[7] The investigator confirmed that the downloaded images contained child pornography and traced the IP address to DeProspero's home.[8] Based on that investigation, the police obtained a search warrant authorizing a search of the defendant's home and the seizure of his computers and electronics, including "keyboards, printers, modems, scanners, or digital cameras and their internal or external storage media."[9] When police officers searched DeProspero's home on May 5, 2009, they discovered a digital image of a female child performing oral sex on a male adult on his computer.[10] The defendant was arrested, and the police seized his computer as well as two digital cameras.[11]

The electronics seized from the defendant's home pursuant to the May 2009 warrant were not promptly taken to the State Police Crime Laboratory for a forensic examination.[12] Mistakenly believing that the only evidence against the defendant was the image of child pornography found on his computer during the search, the Assistant District Attorney ("ADA") offered DeProspero a light prison sentence—six months—and ten years of probation in exchange for his plea of guilty to possession of child pornography.[13] The defendant immediately accepted the offer and was sentenced on November 2, 2009.[14]

After sentencing, DeProspero's attorney contacted the ADA and requested the return of the electronics that were seized during the search of the defendant's home in May 2009.[15] Before returning the defendant's property, however, the ADA instructed the New York State Police to examine it to ensure that it was free of contraband.[16]

---

[6] People v. DeProspero, 932 N.Y.S.2d 789, 791 (App. Div. 4th Dep't 2011).

[7] *Id.*

[8] *Id.*

[9] *Id.* at 791-92.

[10] *Id.* at 792.

[11] *DeProspero*, 932 N.Y.S.2d at 792.

[12] *Id.*

[13] *Id. See also* N.Y. PENAL LAW § 263.16 (McKinney 2013) ("A person is guilty of possessing a sexual performance by a child when . . . he knowingly has in his possession or control, or knowingly accesses with intent to view, any performance which includes sexual conduct by a child less than sixteen years of age.").

[14] *DeProspero*, 932 N.Y.S.2d at 792.

[15] *Id.*

[16] *Id.*

Upon fully examining the contents of the seized property, the police discovered hundreds of pornographic images and videos of children on the defendant's computer, as well as a deleted video clip on one of the defendant's digital cameras.[17] Hundreds of still-frame images were recovered from the deleted video clip, depicting the defendant engaged in oral sex with an autistic male child about twelve years old.[18]

DeProspero was indicted on one count of predatory sexual assault against a child and four counts of criminal sexual acts in the first degree.[19] He sought to suppress the evidence seized from his computer and camera on the grounds that the May 2009 search warrant had expired by the time investigators searched his computer in January 2010.[20] He argued that the warrant was no longer supported by probable cause and that the police lacked jurisdiction to search his computer and camera once the first criminal proceeding against him had terminated.[21]

The Oneida County Court denied the defendant's motion to suppress the evidence recovered from the camera and computer, and determined that the May 2009 search warrant was supported by probable cause.[22] The court acknowledged that this case presented an issue of first impression—whether the delayed analysis of lawfully seized property constitutes an unreasonable search under the Fourth Amendment.[23] However, it concluded that there was "nothing inherently wrong or improper about a delayed analysis or inspection of property that has been lawfully seized."[24] According to the court, the search did not violate the Fourth Amendment because the defendant did not have a legitimate expectation of privacy in the items that were seized from

---

[17] *Id.*

[18] *Id.*

[19] *DeProspero*, 932 N.Y.S.2d at 792. *See also* N.Y. PENAL LAW § 130.96 (McKinney 2006):

> A person is guilty of predatory sexual assault against a child when, being eighteen years old or more, he or she commits the crime of rape in the first degree, criminal sexual act in the first degree, aggravated sexual abuse in the first degree, or course of sexual conduct against a child in the first degree, as defined in this article, and the victim is less than thirteen years old.

Id.

[20] *DeProspero*, 932 N.Y.S.2d at 792.

[21] *Id.*

[22] *Id.* at 793.

[23] *Id.*

[24] *Id.*

his home.[25] Although there was approximately a seven-month delay between the search of the defendant's home and the forensic search of the seized property, the court concluded that "the May 2009 warrant continued to provide probable cause for the subsequent search."[26] Thus, the police had no obligation to obtain a second search warrant in order to conduct a complete forensic analysis of the property seized in May 2009.[27] In other words, the court deemed that the search warrant was valid through, and including, the time the police thoroughly searched the defendant's property.

DeProspero pleaded guilty to predatory sexual assault against a child after the court denied his motion to suppress the evidence.[28] He was sentenced to a term of eighteen years to life and subsequently appealed his conviction.[29] The Fourth Department of the Appellate Division affirmed the conviction, and the defendant appealed to the New York State Court of Appeals.[30]

B. The New York Court of Appeals Decision

The issue presented to the Court of Appeals was whether the January 2010 forensic examination of the defendant's computer and cameras constituted a legal search and seizure.[31] Specifically, whether the authority provided by the May 2009 warrant had expired—and in the absence of new judicial authorization, whether the delayed forensic examination was illegal and the evidence obtained from it inadmissible.[32] The defendant alleged that the prosecution resulting in his September 2009 conviction had run its course and the seized items were no longer useful in that or any other criminal proceeding.[33] Thus, because there was no outstanding criminal matter that needed to be resolved, he argued that the contents of the digital camera had become irrelevant and, as a result, his legitimate expectation of privacy had

[25] *DeProspero*, 932 N.Y.S.2d at 793. *See also* Katz v. United States, 389 U.S. 347, 353 (1967) (providing that Fourth Amendment protections turn on the absence or presence of an expectation of privacy).

[26] *DeProspero*, 932 N.Y.S.2d at 793.

[27] *Id.*

[28] *DeProspero*, 987 N.E.2d at 264.

[29] *DeProspero*, 932 N.Y.S.2d at 793.

[30] *DeProspero*, 987 N.E.2d at 265.

[31] *Id.*

[32] *Id.*

[33] *Id.* at 266.

been restored.[34]

The New York State Court of Appeals rejected the defendant's arguments and upheld the judgment of the Appellate Division.[35] The court began its analysis with the proposition that Fourth Amendment prohibitions against unreasonable searches and seizures are "prevalently understood to protect what an individual may legitimately expect to keep private against unwarranted intrusion by agents of the state."[36] A proponent of a claim for a Fourth Amendment violation must be able to allege a legitimate expectation of privacy in the places or items said to have been illegally searched or seized.[37] In applying this standard, the court found that the defendant in this case had no legitimate expectation of privacy at the time of the forensic examination.[38] Although the initial criminal matter against the defendant had been resolved, the authority of the May 2009 warrant did not vanish at the time of the forensic search. The court explained:

> It is manifest that the continued validity of a search warrant . . . is not necessarily tied to the pendency of any particular prosecution. The duration of a warrant's authority is more appropriately measured by the persistence of the cause for its issue. Here, the predicate for the seizure and examination of defendant's digital media devices was at least as compelling in January 2010 as it had been in May 2009. This being so, there appears no reason to conclude that the warrant did not at the time of the state laboratory examination remain valid and allow both the State's continued custody of the seized property and the "lesser-related intrusion" involved in that property's inspection.[39]

In the court's view, nothing had happened since the seizure of DeProspero's property to "diminish the cause for the warrant's issue."[40] Accordingly, the warrant remained valid at the time of the forensic examination, and the defendant had no relevant expectation of

---

[34] *Id.*

[35] *DeProspero*, 987 N.E.2d at 265.

[36] *Id.* at 266 (citing *Katz*, 389 U.S. at 350).

[37] *Id.* (citing Rakas v. Illinois, 439 U.S. 128, 143 (1978)).

[38] *Id.* at 267.

[39] *Id.* at 266-67.

[40] *DeProspero*, 987 N.E.2d at 266.

privacy protected by the Fourth Amendment.[41]

III. THE FOURTH AMENDMENT AND ITS APPLICATION TO ELECTRONICS

The Fourth Amendment of the United States Constitution protects "[t]he right of the people to be secure . . . against unreasonable searches and seizures."[42] Warrants to execute a search or seizure must be issued "upon probable cause . . . and particularly describ[e] the place to be searched . . . or things to be seized."[43] The Supreme Court has stated that the particularity requirement for a warrant was designed to ensure that "those searches deemed necessary . . . [are] as limited as possible."[44] Furthermore, "[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant [that describes] another."[45] These rules help ensure that the search will be carefully tailored to its justifications and will not result in a general rummaging through a suspect's property.[46]

The dictates of the Fourth Amendment have been consistently applied to searches and seizures for many years. Their application to computer searches, however, is a recent development. With the vast amounts of technological data that can be stored in a computer, commentators have debated that current laws need to be amended so that the Fourth Amendment still protects citizens against overly broad searches.[47] Professor Orin Kerr suggested that applying existing Fourth Amendment principles to digital evidence is a troublesome endeavor.[48] He argued that searching through a computer is roughly

---

[41] *Id.* at 267.

[42] U.S. CONST. amend. IV.

[43] *Id.*

[44] *See* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (describing the underlying rationale for prohibiting the execution of a general or overly broad warrant).

[45] *See* Marron v. United States, 275 U.S. 192, 196 (1927) (describing the Supreme Court's rational behind the particularity requirement).

[46] *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (explaining that the scope of a lawful search is defined by the object of the search and the place in which there is probable cause to believe that it may be found).

[47] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1017 (2010) (discussing how Fourth Amendment protections currently apply to the internet).

[48] *See* Kerr, *supra* note 2, at 289.

analogous to searching for a needle in a haystack,[49] and that new rules must be developed to regulate how investigators look through the haystack to find the needle.[50] While professor Kerr was mostly concerned with overbroad searches, he also addressed the issue of how these overbroad searches result in forensic examinations that take an unreasonable amount of time to complete.[51] Kerr contended that existing rules only focus on a suspect's property interest rather than a suspect's privacy interest.[52] As a result, "the police can keep the [evidence] and continue to search it without apparent limit."[53] According to Professor Kerr, while existing rules may be acceptable for a search of physical property, they reflect a general "[in]attention to the legitimate interests that [a suspect may] have in [his] computer and files."[54]

IV. THE FORENSIC ANALYSIS: A TWO-STEP PROCESS

After a magistrate judge has determined that a warrant application is sufficiently particularized and supported by probable cause, the police will execute the warrant.[55] A search for digital evidence is a two-step process.[56] The first step, known as the "physical search stage," occurs when the police enter the location to be searched and seize the electronic storage devices implicated by the warrant.[57] This on-site seizure commonly includes the confiscation of computers, disks, CD-ROMs, and other electronic devices that may contain relevant evidence.[58] In most cases, agents will either create an "image copy" of the hard drive or seize the electronic devices for a later search of the hardware.[59]

---

[49] *Id.* at 301.

[50] *Id.* ("If no rules regulate how investigators look through the haystack to find the needle, any justification for a search may justify an invasive look through computer files that represent a small city's worth of private information.").

[51] *Id.* at 305.

[52] *Id.* at 306.

[53] Kerr, *supra* note 2, at 306.

[54] *Id.*

[55] U.S. CONST. amend. IV (providing in pertinent part: "[N]o warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized.").

[56] Corey J. Mantei, *Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches*, 53 ARIZ. L. REV. 985, 1006 (2011) (describing the techniques utilized by law enforcement agents for searching a computer's file system).

[57] *Id.*

[58] *Id.* at 1006-07.

[59] *Id.* at 1007.

The second stage, known as the "electronic search stage," occurs when the government conducts a forensic examination of the seized digital storage device.[60] This process almost always occurs off-site (at a police crime laboratory) and is normally executed by specialized computer technicians after the initial physical seizure.[61] The electronic search stage usually requires that the computer be taken off-site to be thoroughly searched because in a majority of cases, forensic analysis of a hard drive takes too long to perform on-site during the initial execution of a search warrant.[62]

Examining a computer for evidence of a crime is a rather time consuming process. Even if the police know specific information about the files they seek, the data may be encrypted, mislabeled, stored in hidden directories, or embedded in "slack space"[63] that may not be discovered absent a full forensic examination.[64] Furthermore, evidence of a crime may not always be located within a file.[65] It may be hidden deep within the computer's data, rendering the evidence extremely difficult to locate and retrieve without the appropriate tools and time.[66] It can potentially take weeks to find the specific information described in the warrant because computer storage devices can contain extraordinary amounts of information.[67] Because examining a computer for digital evidence of a crime is complex and time consuming, it is unrealistic to conduct a thorough on-site search of a computer or any other electronic media device.[68] For these reasons, courts have approved the

---

[60] *Id.*

[61] Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1248 (2010) (describing how computer searches differ from traditional searches).

[62] *Id.* at 1249.

[63] *See* United States v. Moreland, 665 F.3d 137, 142-43 (5th Cir. 2011) (citation omitted) ("Deleted files are not wholly removed from the computer. A deleted file is marked as unallocated file space, which allows that file to be overwritten by new files. A computer's deleted files make up what is known . . . as the disk slack space.").

[64] *See* United States v. Hill, 332 F. Supp. 2d 1081, 1090-91 (C.D. Cal. 2004), *aff'd* 459 F.3d 966 (9th Cir. 2006); *see also* United States v. Gray, 78 F. Supp. 2d 524, 530-31 (E.D. Va. 1999) (noting that criminals intentionally mislabel files or attempt to bury incriminating files within innocuously named directories).

[65] U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 76, *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [hereinafter DOJ MANUAL].

[66] *Id.*

[67] *See Hill*, 459 F.3d at 974-75 ("[T]he officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days.").

[68] In cases involving large quantities of paper documents, courts have traditionally allowed investigators to remove the documents to an off-site location for review to determine

removal of computers to an off-site location for review, but so far have been unable to reach a consensus on the permissible time period for examining seized media.[69]

V. PERMISSIBLE TIME PERIOD FOR EXAMINING SEIZED MEDIA

Statutes that require the timely execution of a search warrant ensure that probable cause still exists at the time of the search.[70] A delay in executing a search warrant may render the probable cause determination stale.[71]

Many courts have agreed that neither the Fourth Amendment nor the Federal Rules of Criminal Procedure place explicit limits on the duration of any forensic analysis and have upheld forensic analyses that were conducted months after investigators lawfully seized a computer.[72] The absence of a specific time period for a forensic examination of electronically stored data is confirmed by the most recent amendment to Rule 41 of the Federal Rules of Criminal Procedure:

> A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the

which of them fall within the scope of the warrant. *See* United States v. Santarelli, 778 F.2d 609, 616 (11th Cir. 1985) (upholding the seizure of an entire file cabinet when such seizure was motivated by the impracticability of on-site sorting).

[69] *See* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (providing that the narrowest definable search and seizure reasonably likely to obtain the evidence described in a warrant is, in most instances, the seizure and subsequent off-premises search of the computer and all available disks); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) ("[T]he affidavit explained why it was necessary to seize the entire computer system in order to examine the electronic data for contraband. It also justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis."). *See also* United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("[U]ntil technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur.").

[70] People v. Kibblewhite, 178 Cal. App. 3d 783, 785 (Dist. Ct. App. 1986).

[71] United States v. Gibson, 123 F.3d 1121, 1124 (8th Cir. 1997).

[72] *See* United States v. Burns, No. 07CR556, 2008 WL 4542990, at *8-9 (N.D. Ill. Apr. 29, 2008) (upholding a ten month delay); United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (upholding a ten month delay); United States v. Hernandez, 183 F. Supp.2d 468, 480-81 (D.P.R. 2002) (upholding a six week delay); United States v. Triumph Capital Grp., Inc., 211 F.R.D. 31, 66 (D. Conn. 2002) (providing that as long as the time was reasonable under the circumstances, a search of weeks or months does not violate the Fourth Amendment).

> warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and *not to any later off-site copying or review*.[73]

This section of Rule 41 was amended in 2009, as courts became aware that computers and other electronic storage media commonly contain such large amounts of information, all of which is impractical for law enforcement to review during execution of the warrant at the search location.[74] However, the amendment still does not impose any rule as to when investigators must begin a forensic examination involving electronically stored information, nor does it impose a time limit or deadline on the duration of such a search:

> [T]he practical reality is that there is no "one size fits all" presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.[75]

For these reasons, the current version of Rule 41 does not place explicit limitations on when the search of the media must occur. As long as the subsequent search is "consistent with the warrant," it is considered valid.[76]

Although Rule 41 does not set forth a specific time period for which seized media may be examined, the Fourth Amendment does require that forensic analysis of a computer be conducted within a reasonable time.[77] In determining the reasonableness of the time for con-

---

[73] FED. R. CRIM. P. 41(e)(2)(B) (emphasis added).

[74] FED. R. CRIM. P. 41(e)(2)(B) advisory committee's note.

[75] *Id.*

[76] *Id.*

[77] *See* United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1077 (D.N.D. 2008) ("[T]he Federal Rules of Criminal Procedure do not require that the forensic analysis of computers and other electronic equipment take place within a specific time limit. Any subsequent search only needs to be conducted within a reasonable time."). *See also Burns*, 2008 WL

ducting a forensic analysis, courts have recognized that the examination of computer data is a difficult and lengthy process.[78] Some courts have treated the dissipation of probable cause as the best indicator of the reasonableness of a search's length.[79] Thus, as long as probable cause to believe that the seized media contains contraband still exists at the time of the forensic examination, the search will not violate the Fourth Amendment.[80]

While the reasonableness requirement is a rather flexible standard governing off-site searches, some courts have attempted to limit the forensics process to prevent a "general rummaging through seized computers."[81] For example, some magistrate judges have begun to issue warrants seeking to seize computers on the condition that the government adheres to certain restrictions on the subsequent search.[82] Some judges have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, such as thirty days.[83] One magistrate judge even refused the government's request for a warrant to search a computer unless the government first agreed to abide by preapproved search methods to ensure that the search was constitutionally reasonable.[84]

Current law does not expressly authorize judges to issue war-

---

4542990, at *8 ("A delay must be reasonable, but there is no constitutional upper limit on reasonableness.").

[78] *See supra* notes 64-69 and accompanying text.

[79] *See* United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005) ("The Fourth Amendment itself 'contains no requirements about *when* the search or seizure is to occur or the *duration*.' However, 'unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant.' ") (citations omitted).

[80] *See* United States v. Brewer, 588 F.3d 1165, 1173 (8th Cir. 2009) (concluding that the delay in forensically analyzing the seized evidence did not have an effect on the probable cause determination); *see also Triumph Capital Grp., Inc.*, 211 F.R.D. at 66 ("Delay in executing a warrant beyond the time set forth in [FED. R. CRIM. P. 41(e)(2)(A)] is not unreasonable unless, at the time it is executed, probable cause no longer exists and the defendant demonstrates legal prejudice as a result of the delay.").

[81] Kerr, *supra* note 2, at 315.

[82] *Id.*

[83] *See* United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (noting that the magistrate judge permitted agents to seize the computers of a child pornography suspect on the condition that the agents searched through the computers for evidence within thirty days).

[84] *See In re* Search of 3817 W. West End, 321 F. Supp. 2d. 953, 955 (N.D. Ill. 2004) (requiring the government to provide a protocol outlining the methods it would use to ensure that its search was reasonably designed to focus on documents related to the criminal activity).

rants that place rigid time restraints on law enforcement's subsequent examination of seized evidence, and whether such limits should be imposed remains an open question—especially in light of the recent amendment to Rule 41.[85] Amidst all the ambiguity regarding off-site searches of electronic data, one thing is perfectly clear—a valid warrant entitles investigators to seize computers and search them off-site at a later date.

VI. FEDERAL APPROACH

Currently, many federal courts apply a "reasonableness" standard in determining if a delay between the initial seizure of the computer and the subsequent search of its data was constitutional.[86] The United States District Court for the Eastern District of New York recently decided *United States v. Metter*, a case that "may impact electronic discovery in future criminal investigations."[87] In 2010, the government indicted the defendant, Metter, and six others, alleging that he had participated in a fraudulent scheme relating to transactions in the common stock of Spongetech Delivery Systems, Inc., a company where he was the president and CEO.[88] Pursuant to a search warrant, the government seized computers from both the Spongetech offices and Metter's home.[89] This included, among other things, sixty-one computer hard drives, the company email server, and contents of Metter's four personal hard drives.[90] With respect to the seized computer hard drives, the government created copies of the data and promptly returned the computer to its appropriate owner, but the government did not conduct a forensic examination of the hard drives until fifteen months after it executed the search warrant.[91]

Metter filed a motion to suppress the seized materials, arguing that "the government's significant delay in conducting off-site searches of the evidence merit[ed] blanket suppression of all seized and imaged evidence" because a delay of fifteen months was unreasonable and would violate the Fourth Amendment.[92] The government's contention

---

85 DOJ MANUAL, *supra* note 62, at 93-94.

86 *See supra* notes 71-77 and accompanying text.

87 860 F. Supp. 2d 205 (E.D.N.Y. 2012).

88 *Id.* at 206.

89 *Id.* at 209.

90 *Id.*

91 *Id*. at 210-11.

92 *Metter*, 860 F. Supp. 2d at 211.

was that the wholesale seizure of hard drives and the subsequent off-site review of such data were necessary given the digital nature of the evidence.[93] With respect to the delay between the seizure and forensic analysis, the government argued that "its prompt return of the original electronic evidence . . . negate[d] any harm arising out of its delayed review of the imaged evidence."[94]

The District Court for the Eastern District of New York began its discussion by noting that this was a case of first impression for the Second Circuit.[95] The question before the court was whether the government's retention of the seized electronics for a fifteen-month span before conducting the forensic search violated the Fourth Amendment's privacy protections.[96] The court determined that the answer to this question required a careful case-by-case factual analysis "because what may be appropriate under one set of facts and circumstances may not be so under another."[97] That being said, the court found that the government's "more than fifteen-month delay" in reviewing the imaged copy of the seized electronic evidence, under the facts and circumstances of this particular case, constituted an unreasonable seizure under the Fourth Amendment:

> An image of an electronic document contains all of the same information as the original electronic document. To the extent the owner or custodian of the electronic document has privacy concerns regarding the government's retention of the original document, the owner would have identical privacy concerns with the government's retention of the imaged document. For example, the seizure of a personal email account could . . . yield personal communications between a cheating spouse and his or her paramour or communications between an individual and his or her family regarding an embarrassing medical condition. These hypothetical communications clearly fall outside the scope of the search warrants in this case . . . . Thus, the government's long-term retention of images of these commu-

---

93 *Id.*

94 *Id.*

95 *Id.* at 212.

96 *Id.*

97 *Metter*, 860 F. Supp. 2d at 212.

> nications presents the same privacy concerns as would the government's retention of the original communications.[98]

However, the court acknowledged that searching a computer for evidence of a crime presents a "complex situation, given the extraordinary number of documents a computer can contain and store and the owner's ability to password protect and/or encrypt files, documents, and electronic communications."[99] Thus, law enforcement should be permitted some flexibility and latitude in reviewing electronic evidence.[100] The correct standard, therefore, in determining whether the government acted appropriately with regard to an off-site forensic search is a flexible one—reasonableness.[101]

Applying this standard, the court found that the government's delay in reviewing the seized evidence was unreasonable under the circumstances.[102] It noted that while numerous cases have held that a several-month delay between the initial seizure of electronic evidence and the *completion* of the government's review of that evidence may be reasonable in some cases,[103] the court found no authority indicating that the government may seize electronic data and then retain that data indefinitely without any plans to *begin* the forensic analysis.[104] Thus, the court found that the government's "blatant disregard for its responsibility" to begin a prompt forensic analysis of the imaged evidence, under these circumstances, was unreasonable.[105]

The United States District Court for the District of Puerto Rico, in *United States v. Hernandez*,[106] also employed the standard of reasonableness in determining whether a delay in the forensic analysis of seized computer data violated the Fourth Amendment. In *Hernandez*, the court noted that "[n]either [Rule 41 of the Federal Rules of Criminal Procedure] nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic exami-

---

98 *Id.*

99 *Id.* at 213.

100 *Id.*

101 *Id.* at 214 (citing United States v. Graziano, 558 F. Supp. 2d 304, 316 (E.D.N.Y. 2008) ("[T]he manner of the execution of the warrant in searching the computer also will be subject to judicial review under a 'reasonableness' standard.")).

102 *Metter*, 860 F. Supp. 2d. at 215.

103 *Id*.

104 *Id.*

105 *Id.*

106 183 F. Supp. 2d 468 (D.P.R. 2002).

nation after it has been seized pursuant to a search warrant."[107] It also recognized that in many cases, the forensic search of the computer takes place at a different location from where the computer was initially seized due to the sheer volume of information contained within the files.[108] According to the court in *Hernandez*, the same principle is applied when a search warrant is executed for voluminous documents.[109] "The documents are seized within the time frame established in the warrant but examination of these documents may take a longer time, and extensions or additional warrants are not required."[110] The examination of the seized documents at a later date does not automatically make the evidence subject to suppression.[111] The rationale that certain searches may be conducted off-site has been extended to include computers.[112] The court in *Hernandez* concluded that because the search of defendant's home took place within the time period specified in the warrant, it was reasonable for the government to take additional time to inspect the images in the floppy disk, especially after already having discovered child pornography in the defendant's hard disk.[113]

Similarly, the court in *United States v. Mutschelknaus*[114] also addressed the issue of whether a delayed forensic search violated the Fourth Amendment. In that case, the defendant, Chad Allen Mutschelknaus, was charged with possessing and distributing materials involving the sexual exploitation of minors.[115] Investigators submitted a warrant application and supporting affidavit to a magistrate judge for permission to search the defendant's residence.[116] The application specifically requested that law enforcement "be allowed to conduct the forensic search of the computer and electronic storage media *after* the execution and return of the search warrant."[117] The judge granted the search warrant and ordered that the search be conducted "on or before

---

[107] *Id.* at 480.
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Hernandez*, 183 F. Supp. 2d at 480.
[112] *Id.* at 480-81 (quoting Commonwealth v. Ellis, No. 97-192, 1999 WL 815818, at *9 (Mass. Super. Ct. Aug. 27, 1999)).
[113] *Id.* at 481.
[114] 564 F. Supp. 2d 1072 (D.N.D. 2008).
[115] *Id.* at 1073-74.
[116] *Id.* at 1074.
[117] *Id.* (emphasis added).

December 22, 2007."[118] The warrant was executed on December 12, 2007, and the forensic analysis of the seized computer was conducted between December 14, 2007, and February 12, 2008.[119]

The defendant filed a motion to suppress the evidence obtained from that search, contending, *inter alia*, that the forensic analysis of the computer and electronic media was an unreasonable search in violation of Rule 41(e)(2)(A) of the Federal Rules of Criminal Procedure because the forensic search "was conducted more than ten days after the issuance of the search warrant."[120] The District Court for the District of North Dakota rejected this argument.[121] Relying instead on the analysis in *Hernandez*, the court held that the Fourth Amendment only requires that the subsequent forensic examination of the computer be made within a reasonable time.[122] The court recognized "that a search of computer data involves much more preparation than an ordinary search . . . and that the search may involve much more information."[123] Applying the reasonableness standard, the court in *Mutschelknaus* concluded that because the computer and electronic media were seized within the time limit established in the search warrant and the forensic analysis took place within the time period granted by the magistrate judge, the evidence would not be suppressed.[124] The court did not limit its holding on the fact that the forensic analysis was conducted within the time period established by the magistrate judge. Instead, the court held that "[*a*]*ny* subsequent search only needs to be conducted within a reasonable time."[125]

The Court of Appeals for the Eighth Circuit affirmed the district court's holding, finding that "[b]ecause of the nature of this evidence, the . . . delay in searching the media did not alter the probable cause analysis."[126] Furthermore, the Eighth Circuit found that the police did not act in bad faith, or "show a reckless disregard for proper procedure."[127] The court recognized that searches of computers take

---

[118] *Id.*

[119] *Mutschelknaus*, 564 F. Supp. 2d at 1074.

[120] *Id.* at 1076.

[121] *Id.* at 1077.

[122] *Id.* at 1076-77.

[123] *Id.* at 1076.

[124] *Mutschelknaus*, 564 F. Supp. 2d at 1077.

[125] *Id.* (emphasis added).

[126] United States v. Mutschelknaus, 592 F.3d 826, 830 (8th Cir. 2010) (alteration in original) (quoting *Brewer*, 588 F.3d at 1173).

[127] *Id.*

longer than ordinary searches and that other courts have permitted the delay in the execution of search warrants involving computers "because of the complexity of the search."[128]

The Eighth Circuit applied the reasonableness standard again in *United States v. Brewer*.[129] In *Brewer*, the court concluded that the delay in forensically analyzing the seized evidence did not have any effect on the probable cause determination.[130] The court stated that the purpose of the Fourth Amendment's unreasonable delay standard is to prevent the execution of a stale warrant.[131] A warrant becomes stale if the information supporting the warrant is not "sufficiently close in time to the issuance of the warrant and the subsequent search conducted so that probable cause can be said to exist as of the time of the search."[132] Important factors that a court should consider in determining whether probable cause has dissipated include the type of the criminal activity involved, the extent of the delay, and whether the seized property is physical or digital in nature.[133] The court in *Brewer* found that the digital nature of the evidence justified the several months' delay in forensically examining the evidence and that such a delay did not alter the probable cause analysis.[134] Probable cause for believing that the media contained child pornography existed at the time the warrant was executed, and therefore, the forensic examination at issue in *Brewer* did not violate the Fourth Amendment.[135]

The United States Court of Appeals for the First Circuit in *United States v. Syphers*[136] also held that a delay in execution of the warrant under Rule 41 did not automatically render seized evidence inadmissible.[137] The First Circuit noted that "[c]ourts have permitted some delay in the execution of search warrants involving computers because of the complexity of the search."[138] The court in *Syphers* held that the five-month delay in examining the appellant's computer did not merit suppression of the seized evidence because the appellant

---

128 *Id.*
129 588 F.3d 1165 (8th Cir. 2009).
130 *Id.* at 1173.
131 *Id.* at 1172-73.
132 *Id.* at 1173 (quoting United States v. Palega, 556 F.3d 709, 715 (8th Cir. 2009)).
133 *Id.*
134 *Brewer*, 588 F.3d at 1173.
135 *Id.*
136 426 F.3d 461 (1st Cir. 2005).
137 *Id.* at 469.
138 *Id.*

failed to demonstrate that the delay altered the probable cause determination or that law enforcement acted in bad faith to evade constitutional requirements.[139]

The reasonableness standard also renders it unlikely that a federal court will impose specific time limitations that would restrain law enforcement's ability to acquire incriminating evidence. For example, in *United States v. Gorrell*,[140] the court rejected the defendant's argument that the data recovered from the computers and camera was inadmissible due to the ten-month delay in processing.[141] The court found that the warrant at issue in *Gorrell* did not limit or specify the time period in which the government was required to conduct its forensic analysis of the seized property and that other courts have declined to impose "such a prophylactic constraint on law enforcement."[142] Thus, although the delay in *Gorrell* was extensive, it did not render the forensic search beyond the scope of the warrant to the extent that the evidence should have been suppressed.[143]

Finally, in *United States v. Triumph Capital Group, Inc.*,[144] the United States District Court for the District of Connecticut held that a "[d]elay in executing a warrant beyond the time set forth in [Rule 41] is not unreasonable unless, at the time it is executed, probable cause no longer exists and the defendant demonstrates legal prejudice as a result of the delay."[145] In *Triumph*, the warrant authorized a forensic search that could have potentially taken weeks or months.[146] The court explained that as long as the time period for the forensic search was "reasonable under the circumstances," such a delay would not be unconstitutional.[147] The court further noted that "neither Rule 41 nor the Fourth Amendment impose any time limitation on the government's forensic examination of the evidence seized."[148] According to the court, "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

---

139 *Id.*
140 360 F. Supp. 2d 48 (D.D.C. 2004).
141 *Id.* at 55 n.5.
142 *Id.*
143 *Id.*
144 211 F.R.D. 31 (D. Conn. 2002).
145 *Id.* at 66.
146 *Id.*
147 *Id.*
148 *Id.*

care in their execution."[149] Thus, the court in *Triumph* concluded that the search in that case was not unreasonable.[150]

Many federal courts decline to impose rigid restraints and time limitations on law enforcement efforts to procure digital evidence from lawfully seized electronics. Indeed, most federal courts agree that as long as a search is reasonable under the circumstances, evidence discovered in a subsequent forensic search of electronic data will generally be admissible. Accordingly, the reasonableness of a search will be determined on a case-by-case basis and will usually depend on many factors, including the nature of the crime, the delay between the initial seizure and the subsequent search, the prejudice to the defendant, the government's good faith, and—of course—whether probable cause still exists at the time of the forensic search.

VII. THE NEW YORK STATE APPROACH

DeProspero presented a novel issue for the New York State Court of Appeals. As the New York Court of Appeals acknowledged,

> neither the Fourth Amendment nor [the New York State Constitution] specifically limit the length of time property may be held following a lawful seizure. Nor is such a limitation evident from the text of New York's statute governing the disposition of evidence obtained by warrant. But the statutory omission is likely no more than a concession to the impossibility of usefully prescribing uniform limitations in this context.[151]

Thus, although the constitutionality of delayed forensic searches is an emerging issue in New York, the court declined to impose uniform time limitations on law enforcement. Consequently, the existence of probable cause seems to be the keystone in upholding the constitutionality of a delayed forensic search.

For example, the continued existence of probable cause was the linchpin of the Monroe County Court's decision in *People v. Loorie*.[152] In that case, the defendants, Debra Loorie and Stuart Sonnendecker,

---

[149] *Triumph Capital Grp., Inc.*, 211 F.R.D. at 66.

[150] *Id.*

[151] *DeProspero*, 987 N.E.2d at 267.

[152] 630 N.Y.S.2d 483 (Sup. Ct. 1995).

were co-owners of the Hilton Pharmacy.[153] The two defendants were indicted for stealing more than $50,000 from the Rochester Area Blue Cross and Blue Shield by billing the two insurance companies for certain drug prescriptions that were not actually supplied to customers.[154] A search warrant was executed, authorizing the police to examine any pharmacy computers and hard drives for evidence relating to the crime.[155] The computer, the backup disks, and several dozen external floppy disks were removed from the premises and were subsequently examined by the police.[156]

The defendants moved to suppress the evidence discovered during the forensic search of the computer.[157] Their primary contention was that law enforcement "exceeded the scope of the warrant" by subsequently examining the contents of the computer's disk drive and floppy disks.[158] They argued that the warrant only authorized law enforcement to *seize* the computer and, therefore, that a second warrant was required in order for the police to search for evidence contained within the hard drives.[159] The question before the court was whether the police were required to obtain a second search warrant explicitly authorizing the search of the contents of the seized computer and floppy disks.[160]

The Monroe County Court began its discussion by acknowledging that "this [was] a case of first impression."[161] Relying on the Supreme Court's decision in *United States v. Ross*,[162] the court in *Loorie* determined that the police did not need to obtain a second search warrant in order to conduct a subsequent forensic examination of the seized property.[163] In *Ross*, the Supreme Court stated,

> A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete

---

153 *Id.* at 484.
154 *Id.*
155 *Id.*
156 *Id.*
157 *Loorie*, 630 N.Y.S.2d at 484.
158 *Id.*
159 *Id.*
160 *Id.*
161 *Id.* at 483.
162 456 U.S. 798 (1982).
163 *Loorie*, 630 N.Y.S.2d at 484-85.

> the search. Thus, a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found. . . . This rule applies equally to all containers.[164]

Drawing upon this language, the court in *Loorie* held that any container[165]—including a hard drive—that is the subject of a properly issued warrant may be thoroughly searched if it is reasonable to believe that it could conceal the type of evidence specified in the warrant.[166] Accordingly, the court held that the police did not exceed the scope of the warrant by conducting a subsequent search of the hard drives because it was reasonable for the police to believe that the disks contained the type of evidence that was the subject of the search warrant.[167] The court concluded that a second search warrant was not necessary for the police to review the items that were lawfully seized.[168]

Similarly, in *People v. Burke*,[169] the defendant, who was charged with numerous sex-related offenses involving children, moved to suppress evidence obtained from his home pursuant to a search warrant.[170] The warrant authorized the police to search Burke's home for evidence of child pornography, including journals, computer disks, and photographic equipment.[171] During the search, the police seized a green metal box containing sexually explicit photographs of children as well as two videotapes.[172] The detectives subsequently examined the contents of the videotapes and discovered that they contained evi-

---

[164] *Ross*, 456 U.S. at 820-22.

[165] A container is defined as any object used for or capable of holding, for transport or storage, such as a carton, box, etc. *Container Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/container?s=t (last visited May 2, 2014).

[166] *Loorie*, 630 N.Y.S.2d at 485. *See also Ross*, 456 U.S. at 824 ("The scope of a warrantless search . . . is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found.").

[167] *Loorie*, 630 N.Y.S.2d at 486. *See also* United States v. Gravitt, 484 F.2d 375, 378 (5th Cir. 1973) ("[W]hen the police take custody of any sort of container . . . it is *reasonable* to search the container to itemize the property to be held by the police. [This reflects] the underlying principle that the [F]ourth [A]mendment proscribes only *unreasonable* searches.") (first emphasis added).

[168] *Loorie*, 630 N.Y.S.2d at 486.

[169] 690 N.Y.S.2d 897 (Sup. Ct. 1999).

[170] *Id.* at 905.

[171] *Id.* at 901.

[172] *Id.*

dence of the defendant engaging in sexual acts with children.[173] The defendant was arrested and charged with numerous counts of sodomy, promoting and possessing an obscene sexual performance of a child, and endangering the welfare of a child.[174]

Burke sought suppression of the videotapes, contending that the search of his home violated the Fourth Amendment.[175] Specifically, the defendant argued that the police were not authorized to examine the contents of the various videotapes.[176] The Kings County Court rejected this argument and denied Burke's motion to suppress the two videotapes.[177] The court first noted that the police are frequently permitted to seize items not specified in the warrant as long as "the warrant authorized the seizure of that *type* of property."[178] According to the court, once the police observed that the videotapes were comingled in a box containing sexually explicit photos, they could reasonably believe that the videotapes also contained evidence of child pornography.[179] The court held that the videotapes were "containers" because they are storage mediums for potentially explicit images, and as such, the police are permitted to search their contents.[180] Also relying on the Supreme Court's decision in *Ross*, the court concluded that, under the circumstances, the police were reasonable in examining the contents of the videotapes to determine whether the tapes contained child pornography.[181]

Other New York cases involving the constitutionality of delayed searches revolved around the defendant's reasonable expectation of privacy. For example, in *People v. Ramirez-Portoreal*,[182] the Court

---

[173] *Id.* at 901-02.

[174] *Burke*, 690 N.Y.S.2d at 899.

[175] *Id.*

[176] *Id.* at 905.

[177] *Id.* at 905-06.

[178] *Id.* at 905 (emphasis added).

[179] *Burke*, 690 N.Y.S.2d at 905.

[180] *Id.* at 905-06.

> Just as the search of the green box was authorized because there was reason to believe that it could contain the specified, illicit photographs, there was reason to believe that the videotape cassettes found in the green box may have served as 'containers'—i.e., a storage medium—for illicit moving images similar in type to the photographs specified in the warrant.

Id.

[181] *Id.* at 906.

[182] 666 N.E.2d 207 (N.Y. 1996).

of Appeals reiterated the basic requirement that in New York, a defendant seeking suppression of evidence must establish "that he or she had a legitimate expectation of privacy in the place or item that was searched."[183] A constitutionally protected privacy interest requires the existence of a subjective expectation of privacy that society is willing to recognize as reasonable.[184] Thus, the reasonable expectation inquiry has both objective and subjective components.

However, privacy concerns are not implicated "when the police simply [look] again at what they had already lawfully seen."[185] The forensic analysis of a blood sample and a forensic analysis of a computer are analogous. In both scenarios, a valid search warrant or subpoena authorizes the seizure of the blood sample or computer. Once such property has been lawfully seized, privacy concerns are no longer relevant because the suspect can no longer reasonably expect the contents of such property to remain private. The seizure of the property necessarily implies that such property will ultimately be searched or examined. The mere fact that the search occurs at a later date is insufficient to restore a legitimate expectation of privacy in the seized item.[186] For example, the New York Court of Appeals in *People v. King*[187] addressed the privacy concerns of a defendant's blood sample after it had been legally seized, but before it was fully examined.[188] The court held:

> It is [] clear that once a person's blood sample has been obtained lawfully, he can no longer assert either privacy claims or unreasonable search and seizure arguments with respect to the use of that sample. Privacy concerns are no longer relevant once the sample has already lawfully been removed from the body, and the scientific analysis of a sample does not involve any further search and seizure of a defendant's person. In this regard we note that the defendant could not plausibly assert any expectation of privacy with respect to the scientific

---

[183] *Id.* at 213.

[184] *Id.*

[185] *See* People v. Natal, 553 N.E.2d 239, 241 (N.Y.1990) ("In that the greater intrusion was justified, . . . the lesser related intrusion [can] not be said to unduly trespass upon any remaining expectation of privacy.").

[186] *See* People v. Perel, 315 N.E.2d 452, 469 (N.Y. 1974).

[187] 663 N.Y.S.2d 610 (App. Div. 2d Dep't 1997).

[188] *Id.* at 614.

> analysis of a lawfully seized item of tangible property, such as a gun or a controlled substance. Although human blood, with its unique genetic properties, may initially be quantitatively different from such evidence, once constitutional concerns have been satisfied, a blood sample is not unlike other tangible property which can be subject to a battery of scientific tests.[189]

Thus, pursuant to *King*, once an item of property is lawfully seized pursuant to a warrant supported by probable cause, the police can take a more detailed look of what they already seized because the defendant no longer has a reasonable expectation of privacy.[190]

In New York, the constitutionality of delayed forensic searches is a contemporary issue that revolves around a rather traditional concept—the expectation of privacy. While establishing the existence of a privacy interest is a prerequisite to a Fourth Amendment challenge, most New York courts agree that such privacy interests no longer exist after a suspect's property has been seized pursuant to a valid warrant. The foregoing cases stand for the proposition that it is permissible for law enforcement to examine the contents of a suspect's seized electronic media at a later date, so long as probable cause existed at the time the property was seized.

VIII. CONCLUSION

People v. DeProspero addressed the growing concern of the effect that emerging technology has on the interpretation and scope of the Fourth Amendment. With new technology underway, courts are forced to analyze the constitutionality of searches and seizures in a new light. While a search for physical evidence is a single-step process, *i.e.*, a home is searched and the evidence is seized, a computer search involves a two-step process by which the computer is seized and then subsequently it is forensically searched for evidence.[191] There is no bright-line test for determining if a delay in forensic analysis results in an unreasonable search. Most federal courts seem to agree that if probable cause still exists, the warrant will still be valid. Furthermore, the amendments that were made to the Federal Rules of Crimi-

[189] *Id.* at 615.
[190] *Id.* at 614.
[191] *See* FED. R. CRIM. P. 41 advisory committee note.

nal Procedure in 2009 address these concerns by declining to impose rigid time restraints on law enforcement agents during the course of a computer search. Although Rule 41 imposes no time restraints on law enforcement officials, this could pose potential problems for the justice system. Time restraints keep a warrant from becoming stale and judges should be encouraged to impose certain restraints, depending on the totality of the circumstances of each case. If a warrant has become stale and probable cause no longer exists at the time of the forensic examination, it may indeed be true that a defendant's legitimate expectation of privacy has been restored and, as a result, any subsequent search would be unreasonable.

It is widely acknowledged that the off-site forensic search of computers takes much longer than an ordinary search, but this does not justify an unreasonable delay in conducting a forensic analysis of seized property. The police and other law enforcement agencies should be required to adequately search the contents of seized items before charging a suspect with a crime, and to do so within a reasonable period of time. While courts should not impose any rigid time constraints on law enforcement, they should address this issue on a case-by-case basis, analyzing all relevant factors and circumstances in order to fairly balance an individual's privacy interest with the state's interest in protecting society from sexual predators.

Paige Bartholomew[*]

[*] J.D. Candidate 2015, Touro College Jacob D. Fuchsberg Law Center; Siena College, B.A. (2012). I would like to thank Professor Gary Shaw and Professor Jeffrey Morris for their guidance and assistance on this case note. I would also like to thank my Constitutional Law Editor, Jared Artura, and the talented members of the *Touro Law Review* for their patience and attention to detail during the editing process. I would like to thank my family and friends, especially Joseph Fritzson, for their continued support and motivation throughout my law school career.