FILE:C:\WINDOWS\DESKTOP\MYBRIE~1\KERRRAW.BK! Dec 12/13/05 Tue 12:52PM

SEARCH WARRANTS IN AN ERA OF DIGITAL EVIDENCE

Orin S. Kerr[*]

ABSTRACT

This Article contends that the legal rules regulating the search warrant process must be revised in light of the demands of digital evidence collection. Existing rules are premised on the one-step process of traditional searches and seizures: the police obtain a warrant to enter the place to be searched and retrieve the property named in the warrant. Computer technologies tend to bifurcate the process into two steps: the police first execute a physical search to seize computer hardware, and then later execute a second electronic search to obtain the data from the seized computer storage device. The failure of the law to account for the two-stage process of computer searches and seizures has caused a great deal of doctrinal confusion, making it difficult for the law to regulate the warrant process effectively. The Article concludes by offering a series of proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure to update the warrant process for the era of digital evidence.

[*] Associate Professor, George Washington University Law School. This paper was commissioned and underwritten by funds from the National Center for Justice and the Rule of Law at the University of Mississippi School of Law (National Center), which is supported by a grant from the Office of Justice Programs at the United States Department of Justice (2000-DD-VX-0032). Thanks to Tom Clancy, Susan Brenner, and Christopher Slobogin for comments on an earlier draft.

INTRODUCTION

Search warrants provide one of the basic tools for collecting evidence in criminal investigations. The history and text of the Fourth Amendment focus heavily on regulating their use.[1] In recent decades, the traditional Fourth Amendment standards governing the warrant process have been supplemented with comprehensive statutory rules such as Rule 41 of the Federal Rules of Criminal Procedure.[2] Today, the combination of statutory and constitutional rules creates a well-defined procedure for obtaining and executing search warrants familiar to every police officer, detective, and prosecutor.

This article argues that the warrant process must be reformed in light of the new dynamics of computer searches and seizures. In the last two decades, the widespread use of computers has led to a new kind of evidence in criminal cases: digital evidence, consisting of zeros and ones of electricity. In a recent essay, I argued that the rise of digital evidence will trigger the need for a "new criminal procedure"—a new set of procedural rules to regulate the acquisition of digital evidence in criminal investigations.[3] This article applies that framework to the warrant process. It explains how the new facts of computer searches and seizures require changes in the laws

[1] See 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."). For a history of the Fourth Amendment and its focus on regulating the warrant process, see NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION (1937).

[2] FED. R. CRIM. P. 41. Each state has equivalent state statutory warrant provisions. See, e.g., CAL. PENAL CODE §§ 1523-42; DEL. CODE ANN. tit. 11, §§ 2304-10 (2005).

[3] Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 COLUM. L. REV. 279, 308 (2005).

governing the warrant process to update that law for the era of digital evidence.

The basic theory is a simple one. The existing law governing the warrant process presumes single-step searches common to the collection of traditional physical evidence. In these cases, the investigators enter the place to be searched, seize the property named in the warrant, and leave. With computer searches, however, the one-step search process is replaced by a two-step search process. The investigators enter the place to be searched; seize the computer hardware; take the hardware off-site; and then later search the equipment for data that may be evidence of crime.[4] Two searches occur instead of one. The physical search comes first and the electronic search comes second. Further, in most cases the two searches are quite distinct. They occur at different times, in different places, and are usually performed by different people.

The division of the traditional one-step warrant process into two distinct steps sets up four doctrinal puzzles for the law regulating the warrant process. First, what should the

[4] See, e.g., In re Search of 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) [hereinafter West End] ("[I]t is frequently the case with computers that the normal sequence of `search' and then selective `seizure' is turned on its head. Because of the difficulties of conducting an on-site search of computers, the government frequently seeks (and, as here, obtains), authority to seize computers without any prior review of their contents."). As Susan Brenner and Barbara Frederiksen have written,

> In conventional searches and seizures, the execution of a warrant typically involves two stages: a "search" for evidence that is followed by the "seizure" of evidence once it has been found. . . .
>
> In off-site computer searches, the execution of a warrant involves four stages, not two: a search designed to locate computer equipment; the seizure of that equipment and its removal to another location; a thorough search of the contents of the equipment which is conducted at that location; and a seizure of relevant evidence located in the course of that search.

Susan W. Brenner & Barbara A. Frederiksen, Computer Searches And Seizures: Some Unresolved Issues, 8 MICH. TELECOMM. & TECH. L. REV. 39, 82 (2002).

warrant describe as the property to be seized: the physical hardware seized during the first physical search, or the digital evidence obtained during the electronic search? Second, what should the warrant describe as the place to be searched: the location of the hardware, the hardware itself or the location where the electronic search will occur? Third, when must the electronic search occur: Is the timing governed by the same rules that govern the physical warrant execution, by some other rules, or by no rules at all? Finally, what record-keeping requirements apply to the electronic search and when must seized computer equipment be returned? All of these questions follow from an attempt to fit the one-step framework of existing law into the two-step framework of the new facts of computer searches and seizures.

This article urges legislatures and rules committees to update the statutory rules that govern the warrant process in response to the new challenge of digital evidence searches. It contends that warrant rules should be amended to recognize the two-step nature of computer searches and seizures and to regulate both steps adequately and directly. Existing law requires courts to try to squeeze the two-step digital warrant process into a one-step legal framework. The courts have struggled to answer the four doctrinal puzzles and often have failed to reach coherent or satisfactory answers. Statutory rule reform is needed to resolve these difficulties and directly address the considerable policy questions they raise.

Two proposed changes are the most important. First, the law should require warrants seeking digital evidence to state the items to be searched for at *both* the physical *and* the electronic search stages. That is, the warrant should state the physical evidence that the police plan to seize at the physical stage and the electronic evidence that the forensics analysts plan to search for at the electronic stage. Second, warrant rules should be amended to require that the electronic search step proceeds in a timely fashion. Specifically, the law should require investigators to "image" seized computers and return the equipment in a reasonable period of time (such as thirty

days) when the hardware is merely a storage device for evidence. When the hardware is believed to be contraband or a fruit or instrumentality of crime, investigators should be required to begin the forensic process within a specific period of time (such as sixty days) to establish whether that belief is correct. If it is not, the hardware should be returned; if it is, investigators should be permitted to retain it.

I will develop my argument in four parts. Part I explores the factual differences between how investigators typically execute a search warrant for digital evidence and how investigators typically execute a warrant for physical evidence. In a traditional case, the police enter the place to be searched, and then locate and retrieve the items found in the warrant. Computer searches follow a different model. Because the retrieval of digital evidence requires technical expertise and considerable time, the execution of a warrant for digital evidence generally involves two steps. The first is location and retrieval of the physical storage device that investigators believe contains the digital evidence, and the second is subsequent analysis of the storage device to locate the digital evidence. Instead of search and seizure, the process is more like physical search and seizure followed by electronic search and seizure.

Part II explores the four doctrinal puzzles created by the bifurcation of the one-step warrant process into two distinct steps. Should the property to be seized be the physical evidence seized at step one, or the electronic evidence searched for at step two? What is the place to be searched: the location of the physical storage device, the storage device itself or the location of the electronic search? When must the search be executed? In particular, what timing rules govern the computer forensic analysis required to execute the electronic search? Finally, what record-keeping requirements apply to the electronic search, and when (if ever) must seized computer hardware be returned?

Part III explores how courts have attempted to resolve these puzzles using existing statutory and constitutional rules. It focuses on the two primary questions that courts have con-

sidered in detail: the proper description of the property to be seized, and the timing of the computer forensic process. Courts have struggled in both areas to fit the old law to the new facts. They have approved both physical and virtual descriptions of the property to be seized, but only by letting the practical considerations of the two-step search override what would otherwise be significant defects in computer warrants. They have also failed to settle whether existing statutory law permits judges to condition warrants on the timing of the forensic process.

Part IV offers a series of specific amendments to the legal framework regulating the warrant process. It explains why the primary changes needed are statutory, not constitutional. The solution to the problem lies in amending of the statutory rules regulating the warrant process, not in altering Fourth Amendment standards. It also offers specific changes to Rule 41 and their state equivalents, including changes in how computer warrants are written and explicit regulation of the timing of the electronic search process when undertaken pursuant to a warrant.

I. DIGITAL VERSUS PHYSICAL WARRANT PROCESSES

The premise of my argument is that the facts common in digital evidence searches are different from the facts common in traditional physical evidence searches. Changes in the facts demand changes in the legal rules. This section introduces those differences, focusing on the replacement of the search-and-retrieve mechanism of traditional searches with a two-stage process that adds an electronic search to the traditional physical search and seizure. In physical searches, the investigators seek permission to look through a particular physical space for a particular piece of evidence, and then to take that evidence away. Executing a warrant for digital evidence generally adds a step. The investigator seeks permission to search a physical space for computer storage devices, and then takes away the computer storage devices that are found for analysis off-site at a later date. Weeks or even months later, the computer forensic analyst performs what is, in a sense, a second search: an electronic search for digital evidence, occurring long after the physical search for physical evidence. The dynamic is physical search, physical seizure, and then electronic search.

The following hypothetical cases explains the dynamic. The first presents a traditional investigation for physical evidence; the second presents a typical investigation for digital evidence. The contrast helps reveal how the basic process of executing a warrant for physical evidence is different in a number of ways from the process of executing a warrant for digital evidence.

A. Physical Searches and Physical Search Warrants

Fred Felony is low on cash, so he decides to burglarize the home of Mr. and Mrs. Smith at 123 Main Street. One night when the Smiths are away, Fred picks the lock to the front door using locksmith tools and starts looking around for valuable property. Fred finds and takes three valuable items: an expensive stereo system, a collection of Victorian gold jewelry, and a mink fur coat. Fred takes these items back to his apartment and hides them in his bedroom closet. Then he puts his locksmith tools in a storage area underneath his kitchen sink. Fred's plan is to wait a few weeks until no one is looking for the stolen items and then to try to sell them at a local pawn shop.

The next day, the Smiths come back into town and realize that their home has been burglarized. They call the police. Imagine you are the police detective called to investigate the burglary at 123 Main Street. You arrive at the scene and quickly surmise that the front door was opened using locksmith tools. You speak to the Smiths, who report that three items have been stolen: a collection of gold jewelry, Mrs. Smith's mink coat and an expensive stereo system. You obtain detailed descriptions of these missing items, including the serial numbers of the stolen equipment and photographs of the stolen jewelry, and you then return to the police station.

Now imagine that you have good reason to believe that Fred Felony was behind the burglary, and that you also know that Fred Felony's last known address is 13 Prospect Avenue, Apartment B. You decide to apply for a search warrant to search Fred's apartment for the stolen goods. If you can find the stolen goods and the locksmith tools in Fred's apartment, you will have very strong evidence of Fred's guilt that can be used in court. You therefore apply for a warrant to search 13 Prospect Avenue, Apartment B for four items: locksmith tools, the mink fur coat, a stereo with the serial numbers of the stolen equipment, and Victorian gold jewelry matching the

description that the Smiths gave you. In the affidavit to the warrant, you explain to the judge why you have probable cause to believe that evidence of the burglary will be located inside the apartment.

The judge finds probable cause and signs the warrant authorizing the search. The next morning, several officers join you in executing the search. You knock on Fred's door at 10:00 a.m. and announce, "This is the police! We have a warrant—open up!" Fred is not home, so after a brief wait the door is forcibly opened. After ensuring that the apartment is empty, you begin to search the home for the evidence in the warrant. After about ten minutes, one officer finds a set of locksmith tools in the storage area under the kitchen sink. The tools are "bagged and tagged," placed in an evidence bag and labeled appropriately. Twenty minutes later, you are looking through the bedroom and open the closet door. You immediately spot the fur coat and stereo equipment. You pick up the equipment and find the serial number to confirm the matching number on the warrant. You then look through the rest of the closet and find the collection of gold jewelry described in the warrant. You bag and tag the jewelry, coat and stereo equipment. With all of the evidence found, you leave a copy of the warrant on the front door so that Fred will know what happened when he returns home. The next day, you file a return with the judge who issued the warrant reporting everything seized from the apartment: the locksmith's tools, fur coat, jewelry, and stereo equipment.

B. Digital Searches and Digital Search Warrants

Now imagine a cyber version of the same crime. This time, Fred decides to commit his crime via his computer. Instead of breaking into the Smiths' home, he decides to hack into their home computer remotely to steal credit cards and other valuable financial information. Fred logs on to the Internet from his computer at home, hacks into the Smiths' home computer, and then locates and retrieves the Smiths' credit card numbers. Fred copies the files from the Smiths' computer, and later uses the Smiths' credit card number to purchase an expensive stereo, a mink coat and some gold jewelry. When the Smiths get their credit card bill weeks later, they see the extra charges and call the police. Once again, you are the investigator called to investigate the crime. Assume that you have reason to believe that Fred Felony is behind the scheme, and you suspect he hacked into the Smiths' computer to obtain the credit card information. Once again, you want to recover the fruits of the crime: the stereo, jewelry, and mink coat.

But this time you also want something else. You want to recover the digital evidence that can prove Fred hacked into the Smiths' computer. If Fred did hack into the Smiths' computer, the computer Fred used should have clues of the crime. Granted, you cannot be sure of exactly what evidence the computer will contain. Perhaps you will find hacker tools establishing Fred's ability to commit the crime. Perhaps you will find the file containing the credit card numbers that Fred copied from the Smiths' computers. Or perhaps you will find a word processing file in which Fred wrote down the steps he took to hack into the Smiths' computer. At this point you cannot know. At the same time, there is a good chance that Fred's computer contains evidence of his hacking crime. The only way to find out is to look for Fred's computer and analyze it for evidence.

Once again, you apply for a warrant to search 13 Prospect Avenue, Apartment B. Once again you want to seize a fur coat,

gold jewelry, and expensive stereo equipment. This time, however, you also request permission to take Fred's computer. You knock on Fred's door, enter the apartment, and quickly find the stereo equipment, fur coat, and jewelry. This time you also look for Fred's computer. To your surprise, however, you end up finding not one but several computers and storage devices. You find one laptop computer in the living room, a desktop computer in the bedroom, and a box of floppy diskettes and thumb drives next to the desktop computer. The number of computers and storage devices give you pause. You don't know which computer is Fred's, or which computers or diskettes (if any) may contain the evidence you are looking for. Given that you can't tell what is on the computers and storage devices without turning them on and looking through them, you decide out of an abundance of caution to call headquarters and ask to speak with a computer expert.

The computer expert tells you that, as a practical matter, you have no choice but to take all of the computers and storage devices with you and send them to a government lab for analysis. He explains that you should not turn the computers on: turning them on will alter the evidence they contain.[5] To avoid altering the evidence on the computers, he explains, a computer forensic analyst must copy each storage device using special forensic tools and conduct a sophisticated and generally time-consuming forensic analysis.[6] The computer expert also emphasizes that it can take many hours, or even days, to locate specific evidence on a computer hard drive. It is technically possible to send an expert to 13 Prospect Avenue and have him try to search the computers on-site, he explains, but it is likely to be quite time consuming. Outside of the controlled environment of a government forensic lab, he cannot

[5] See, e.g., U.S. DEPT. OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 24 (2004), available at http://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[6] See BILL NELSON, ET. AL, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS (Thomson 2004).

guarantee that the evidence will be located properly. This won't do, you realize. You need to find the evidence, and you can't spend the next few days sitting in Fred's apartment with a technical expert looking through Fred's computers. The most practical option seems to be to "bag and tag" all of the computers and hard drives and let the technical experts figure it out later. You do that, and the next day you file a return on the warrant with the judge listing the evidence you seized: first, the stereo equipment, fur coat and jewelry; and second the laptop computer, desktop computer, and the box of floppy diskettes and thumb drives.

While the search of Fred's apartment is now complete, you are not done. You now need to send the computers and disk drives to the local government forensic lab for analysis. You ship the equipment to the lab, and wait for a response. After you don't hear back for a few weeks, you call the laboratory and ask if they have looked at your computers yet. The lab technician explains that the forensic process is very time consuming and that there is a three-month waiting list before a computer brought to the lab will be analyzed.[7]

Several months later, you receive a call that the analysis has been completed. A computer forensic analyst performed an analysis of the various hard drives and storage devices, which required him to generate copies of each of the computer drives and perform various computer commands on the copies to try and locate the evidence they contained.[8] The technician's report informs you that the analyst found evidence of a hacking incident on one of the computers. The evidence includes hacker tools that could have been used to hack into the Smiths' computer, as well as a copy of the stolen file that contained the credit card numbers taken from the Smiths' computer. The other computer and the additional storage devices did not

[7] Such delays are typical, although the actual delay may vary tremendously from case to case.

[8] I explain the computer forensics process in detail in Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. (forthcoming Dec. 2005).

contain any evidence of criminal activity.

II. FOUR PUZZLES: DIGITAL EVIDENCE AND THE INADEQUACY OF EXISTING LEGAL RULES

With the basic differences between physical evidence and digital evidence searches in mind, let's next consider how existing law regulates the two types of searches. This section illustrates how the law regulating the warrant process is attuned to the basic mechanisms of physical searches. Existing rules were designed to regulate the collection of physical evidence, and are naturally tailored to the search-and-retrieve dynamic. Application of the same rules to digital evidence cases reveals that the law no longer fits the facts. A series of doctrinal puzzles emerges, requiring investigators and judges to adjust the rules as best they can to come up with alternatives. This section explores the clash between the traditional rules and the new facts by exploring those existing rules and seeing how they apply to digital evidence warrants.

At the outset, it is important to understand the basic rules of the warrant process. The basic constitutional principle shaping the warrant process is that investigators must execute narrow warrants limited by the scope of probable cause.[9] Investigators can obtain a search warrant only if they have probable cause to believe that evidence, fruits of crime, contraband or instrumentalities of crime are located in a particular physical place.[10] The warrant must name the particular prop-

[9] See Maryland v. Garrison, 480 U.S. 79, 84 (1987). Garrison explains:

> By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. Thus, the scope of a lawful search is [] defined by the object of the search. . . .

Id. (footnote omitted).

[10] Id.

erty that the police have probable cause to believe will be located in the particular place to be searched.[11] Investigators can then obtain a warrant authorizing them to go to the particular place named and search for and seize that particular property.

These constitutional rules are supplemented by statutory rules, such as Federal Rule of Criminal Procedure 41.[12] Rule 41 specifies what judges can issue warrants; what form the warrants must take; what time of day warrants must be executed; how long the police have to execute the warrant; and for what kind of property warrants can be issued. Rule 41 is often quite specific. For example, Rule 41(d) contains relatively detailed rules that govern making an inventory of the property taken and informing the suspect and the court of what was taken:

> The officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property taken or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken. The inventory shall be made in the presence of the applicant for the warrant and the person from whose possession or premises the property was taken, if they are present, or in the presence of at least one credible person other than the applicant for the warrant or the person from whose possession or premises the property was taken, and shall be verified by the officer. The federal magistrate judge shall upon request deliver a copy of the inventory to the person from whom or from whose premises the property was taken and to the applicant for the warrant.

Rule 41 also provides a mechanism by which a suspect can

---

11 Id. at 84-85.

12 FED. R. CRIM. P. 41 (reprinted in Appendix).

13 Id. 41(d).

move for the return of property unlawfully seized.[14] The police have a right to retain the property permanently, however, if it is contraband, a fruit or instrumentality of crime. If the property is mere evidence, they generally can retain it so long as there is a plausible claim of law enforcement need.

These constitutional and statutory rules work quite naturally in the case of physical evidence. This is true for two basic reasons. First, the rules fit the facts of searches for physical evidence. Physical searches generally follow a search-and-retrieve dynamic. Physical evidence generally can be identified and retrieved from a physical place in a matter of minutes or hours. The warrant authorizes the police to enter the physical property, locate, and then retrieve the evidence named in the warrant.[15] In Fred Felony's first hypothetical, for example, the police could enter Fred's apartment and look for the mink coat, stereo equipment, jewelry and locksmith tools. Once they found those items, the investigators could take them away but had to stop searching.

The second reason these rules work with physical evidence searches is that they ensure that the police obtain physical property in a relatively narrow way that minimizes the intrusion onto the suspect's property and privacy. Each of the basic rules attempts to limit and channel police conduct based on the facts of how physical searches for physical evidence work. The particularity requirement limits *where* the police can search. They can only search the physical premises named in the warrant, such as Fred's apartment. The probable cause requirement and statutory rules on executing warrants limit *when* the search can occur; excessive delay may lead the warrant to become stale, and statutory rules govern the time windows in which the search can occur. The particularity requirement of what property is to be seized governs *how* the search occurs; general rummaging through the target's property is not permitted. Finally, a number of the statutory rules add record-keeping

---

[14] Id. 41(g).

[15] See Appendix.

requirements designed to facilitate oversight and judicial review, such as the requirement that an inventory of the property be taken, the filing of a return with the court, and the allowance for motions to return physical property.

A very different picture emerges when we try to apply the existing law to the facts of digital evidence cases, such as the second hypothetical case involving Fred Felony's hack into the Smiths' computers. While the existing rules work well for physical evidence, they raise a number of puzzles when applied to digital evidence. Fitting the two-stage warrant process of digital evidence cases into the single-stage approach of existing law generates four distinct problems: defining the evidence to be seized; defining the place to be searched; regulating the timing of the warrant process; and facilitating judicial review of the warrant process.

A. What is the Evidence to Be Seized?

Consider the first puzzle: how can investigators draft the warrant so that it particularly describes the "things to be seized?" It is a basic tenet of Fourth Amendment law that the "thing to be seized" named in the warrant is the item that the police have probable cause to believe constitutes evidence, a fruit or instrumentality of crime, or contraband. If a piece of computer hardware is known to be contraband or an instrumentality of crime, this tenet may be easy to satisfy. For example, a computer used to hack into another computer is an instrumentality of crime; likewise, a computer used to store child pornography is both an instrumentality of crime and contraband.[16] In these cases, the warrant can name the computer hardware itself. But what if the computer is merely a storage device for evidence, or the police do not know if a particular computer is in fact an instrumentality of crime or contraband? What should the warrant describe as the evidence to be seized?

[16] See U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS app. F at 198-217 (2000),

There are two basic choices, corresponding to the two stages of the warrant process for digital evidence. The first choice is to describe the evidence to be seized as the physical storage devices — the computers themselves. Of course, investigators will not know exactly what those computers look like before they execute the search. In Fred Felony's case, for example, the most specific description the police likely could use would be something like "any computers, computer equipment, diskettes, CD-ROMS, or other electronic storage devices." While not terribly particular, this approach does describe accurately the evidence to be seized in the initial physical search. If you focus on that initial stage, the warrant will be accurate; the police will execute the warrant by entering the place to be searched and looking for (and then retrieving) the physical computers and other storage devices.

The second choice is to describe the evidence to be seized as the digital evidence itself – the electronic data. In the case of Fred Felony's hack, the warrant could state that it authorizes the seizure of "files containing the Mastercard number 2626 2727 2838 1812, or other evidence relating to Mr. and/or Mrs. John Smith of 123 Main Street." This approach does not describe accurately what the police will do on-site, but it does describe the evidence sought at the second stage of the warrant process—the off-site electronic search. If you focus on the latter stage instead of the former, the warrant will be accurate; a forensic expert will execute the warrant by looking through the computers for specific evidence.

Neither choice fits the traditional Fourth Amendment rules particularly well. Describing the things to be seized as the physical storage devices creates two problems. First, the warrant becomes overbroad. The police do not have probable cause to seize every computer storage device located on the premises. Rather, they have probable cause to believe that those computers contain some kind of digital evidence of the crime. Naming

available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf [hereinafter DOJ MANUAL].

the items to be seized as the physical storage devices may be technically accurate at the first stage, but it also means that the warrant itself is no longer as particular as the scope of probable cause. Second, the warrant says nothing (either implicitly or explicitly) about the later search through the computer for the digital evidence. When the forensic experts look through the computer for evidence described in the warrant, they will have nothing to guide them. The warrant will merely say it authorizes the seizure of computer storage devices.

Equivalent problems arise if the warrant describes the particular files as the things to be seized. On one hand, this approach cures the overbreadth problem; the warrant is now much more particular. On the other hand, focusing on particularity creates a new problem. The warrant no longer describes accurately how the initial stage of the warrant will be executed. The warrant authorizes the search and seizure of specific files and data, but the investigators plan to seize all the hardware they can find on-site and send it to a lab for analysis. The execution of the warrant will no longer track what the warrant itself authorizes. Another technical problem is that copying a computer file does not actually "seize" it. As a result, the seizure that occurs is of the device holding the data rather than the data itself.[17] In effect, the police face a choice about what Fourth Amendment error they want to introduce. If they list the evidence to be seized as the physical device, then the warrant will be overbroad; if they list the evidence to be seized as the digital evidence, then the warrant no longer authorizes the police to do what they plan to do.

[17] See Kerr, supra note 8 (citing Arizona v. Hicks, 480 U.S. 321 (1987)).

B. What is the Place to be Searched?

Although this issue arises less frequently, similar problems can arise when investigators attempt to describe the place to be searched. Digital evidence may be stored on a network or located inside an already seized computer stored in government custody. When either of these situations occur, the police may not need authorization to enter the place where the evidence is located. In such cases, what is the place to be searched?

In traditional cases, investigators simply list the location of the physical search as the location where the warrant will be executed. For example, if the police plan to search Fred Felony's apartment at 13 Prospect Avenue, Apartment A, they will list Fred's apartment as the place to be searched. However, this is only the location of the physical search, not the electronic search. In some cases, however, the latter may be more important. For example, a number of decided cases involve warrants authorizing the search of computers already seized and in law enforcement custody.[18] In these cases, the physical search and seizure has already occurred. The police already have the computer, and the warrant is needed only to authorize the electronic search. In such a case, how can the police satisfy the Fourth Amendment's requirement that the warrant specify the place to be searched? Should they list the place to be searched as the physical location of the storage device, such as "storage locker #7 in the Seventh Precinct?" Or, should they list the computer itself, such as "a Dell personal computer with Serial Number X10-23533"? The former satisfies the traditional need to specify the physical location of the search, but in a purely formalistic way; the latter is more accurate, but does not attempt to name a "place" to be searched.

The problem has particular importance in the case of data

[18] See, e.g., United States v. Gray, 78 F. Supp. 2d 524, 530-31 (E.D. Va. 1999) (involving a second warrant obtained to search a computer already in law enforcement custody).

stored remotely on a computer network. Imagine that the police plan to execute a warrant to find a particular e-mail stored on a computer network by logging on to the network (or having an employee of the network operator do so) and retrieving the information remotely. Is the place to be searched the location of the police or the evidence? If the place to be searched is the location of the police when they log on to the network, police can engage in forum-shopping. Depending on how the network is configured, the police may be able to access it from anywhere. If the place is where the individual file is stored, on the other hand, it may stymie investigations. Investigators may be unable to know ahead of time where the evidence is located, and the retrieval of evidence may involve a search outside the United States where no warrant can be obtained.[19]

[19] Cf. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001) (remote search of Russian server from United States).

C. When Can the Search be Executed?

The third question concerns the timing of the second search. Statutory rules governing the warrant process generally lay out a specific time frame for executing the warrant. For example, Rule 41 states that the warrant must be executed "within a specified period of time no longer than 10 days"[20] after the warrant has been signed, and that the search must be executed only between the hours of 6:00 a.m. and 10:00 p.m.[21] It also states that the person who executes the warrant "must enter on its face the exact date and time it is executed."[22] These timing requirements appear reasonable and appropriate in the case of a search for physical evidence. The Rules ensure that Officers do not wait until the probable cause becomes stale, that they do not invade people's homes in the middle of the night, and that they leave a record of the exact time that the warrant was executed. The same requirements apply reasonably to the physical-search stage of the two-stage warrant process for physical evidence. But they leave open a question: what rules apply to the timing of the second stage, the electronic search?

The existing rule leaves open only two possibilities, neither of which is particularly appealing. The first possibility is that the timing requirements of Rule 41 also apply to the electronic search. Under this approach, the computer forensic process must be completed within ten days of the issuance of the warrant, and can be performed only between the hours of 6:00 a.m. and 10:00 p.m. This proves an impossible standard to meet in practice. As we saw in the hypothetical with Fred Felony's computers, the forensic process typically takes a number of days once started, and the backlog of cases in most jurisdictions means that weeks or months may pass before the analysis even begins. Nor does this approach make much sense. While it is

---

20 FED R. CRIM. P. 41(e)(2)(A).

21 Id. 41(a)(2)(B).

22 Id. 41(f)(1).

desirable for electronic searches to occur quickly, staleness is not a concern after the container of evidence has been seized. In addition, there is no reason why a forensic examiner working in the laboratory at night has to stop at 10:00 p.m. or cannot come in to work before 6:00 a.m.[23]

However, the second possibility is also problematic. The electronic search process may simply be exempt from Rule 41's timing requirements. If Rule 41 is construed in this way, nothing requires government investigators to begin or complete the forensic analysis at any time. Investigators can take all of the target's computer equipment and hold them for months or even years, without even beginning the forensic process. This is particularly problematic given that some computers seized may not contain any evidence. In the hypothetical case of seizing Fred Felony's computer, the investigators found two computers and multiple additional storage devices. When the electronic search was executed months later, however, it turned out that only one of the computers contained evidence. This means that the other computer and storage devices ideally would not have been seized in the first place; a rule allowing the police to hold a target's computer until they get around to searching it (however long that may be) seems unfairly insensitive to the legitimate needs of computer owners. The existing Rule 41 is simply ill-prepared to handle the two-stage search process of digital evidence cases, as it forces the second step either to fit within the rules of the first or follow none at all.

[23] That is, other than the Fair Labor Standards Act of 1938, 29 U.S.C. § 207 (2000).

D. What are the Oversight and Record-keeping Requirements, and When Must Property be Returned?

The final issues involve oversight and review of the warrant process, and include the rules that govern when seized property must be returned. Traditional rules require the officer who executes the warrant to create an inventory of the items seized and to provide the judge the inventory list of property seized.[24] The rules then place a burden on the aggrieved property owner to file a motion in court for return of the property.[25] Under Rule 41, the court generally will order the return of the property only if the police no longer have a legitimate claim that they need it for an investigation.[26]

These rules prove awkward in the case of digital evidence searches. First, it is unclear whether the record-keeping requirements refer only to the initial physical search or also include the subsequent electronic search. For example, should the required inventory list include only the physical evidence taken at the first stage, or should it include a list of the computer programs and files that the computers are later revealed to contain? Requiring investigators to generate a quick analysis of the files is impractical given the time-consuming nature of the forensic process; further, owners of computer equipment ordinarily should know what files their computers contain and should not need the police to tell them. If the inventory relates only to the physical evidence, however, then the existing rules do not require any record-keeping for the subsequent electronic search. Once again, applying the initial search rules to the electronic search proves difficult, while declining to apply them leaves an important step of the warrant process unregulated. Similarly, who should receive the inventory list in the case of a computer already in government custody? If the government

---

24 See FED. R. CRIM. P. 41(f)(4).

25 Id. 41(g).

26 See infra note 116.

has a computer in its custody and obtains a warrant to search it, does it need to find the owner of the computer and serve the inventory list on the owner?

The second difficulty concerns the return of property. Computer searches often require investigators to seize all of the computers and storage devices that they find on-site and remove them for subsequent analysis. In many cases, only some of those computers and storage devices will actually contain evidence of the crime; in some cases, none of them will. We saw this problem in the Fred Felony hypothetical. When the investigator entered Fred's apartment, he found several computers and did not know which one contained the evidence he needed. As noted earlier, the investigators often will not realize which computers contain the necessary evidence until many months later when the computers are finally analyzed. Under the current version of Rule 41, however, a property owner simply must wait until the government gets around to looking at the computer. Existing rules simply were not designed for a two-step search environment that begins with a broad seizure. As a result, the rules show little attention to the needs of property owners who may need equipment back for reasons unrelated to the investigation.

III. EXISTING LAW APPLYING THE WARRANT PROCESS TO SEARCHES FOR DIGITAL EVIDENCE

Courts have provided tentative answers to two-and-a-half of the four puzzles raised by the application of the warrant process rules to searches for digital evidence. The one puzzle that has not been addressed at all is how to define the "place to be searched." This issue simply has not yet come up in litigation. Also, only a small amount of litigation has focused on the record-keeping requirements and the rules governing the return of seized computers. Two other steps have been the subject of extensive litigation. The most frequently litigated issue relates to how to describe the evidence to be seized. In the last three years, there has also been a growing body of caselaw on the timing of the search. This section reviews the existing caselaw in order to frame the normative reform proposals that will be made in Part IV.

A. The Things to be Seized

Courts generally have deferred to the government's choice of whether to describe the property to be seized as the computer hardware or the digital evidence itself. Both approaches have been upheld, at least within limits; no court has required that the police use one approach or the other. This does not mean that courts have rubber-stamped the government's work. Rather, they have scrutinized both approaches and concluded that, within reason, the government can chose which approach to use. The courts' approval of both strategies owes in large part to a practice followed by many investigators (and recommended by the Department of Justice) of explaining the need for the two-stage search process in the warrant affidavit. This practice uses the affidavit as a way to communicate the details of the search process to the judge; by signing the warrant, the court in effect approves the two-step search process. At least some courts have suggested that this practice effectively cures what otherwise could be an inherent constitutional defect in the two-stage search for digital evidence.

The more common practice has been to describe the evidence to be seized as the physical computers. An example of a decision upholding such a practice is *United States v. Upham*.[27] In *Upham*, agents investigating a child pornography case obtained a warrant to seize "[a]ny and all computer software and hardware, . . . computer disks, [and] disk drives."[28] Judge Boudin rejected the defendant's claim that the seizure of "all computers" was overbroad:

> As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was

---

[27] 168 F.3d 532 (1st Cir. 1999).

[28] Id. at 535. The warrant in Upham also named the evidence itself: "[a]ny and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]." Id. However, the court resolved the challenge, by relying only on the first description. Id. at 536.

> about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs. We conclude, as did the Ninth Circuit in somewhat similar circumstances, that the . . . [language] was not unconstitutionally overbroad.
>
> Of course, if the images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of all computer equipment, a category potentially including equipment that contained no images and had no connection to the crime. But it is no easy task to search a well-laden hard drive by going through all of the information it contains, let alone to search through it and the disks for information that may have been "deleted." The record shows that the mechanics of the search for images later performed off site could not readily have been done on the spot.[29]

Note that Judge Boudin looked to the practical needs of law enforcement to determine whether the warrant was overbroad, rather than to the scope of probable cause. Because the government had made the case that it needed to seize all computers for practical reasons, it was not overbroad for the warrant to reflect this on its face.[30]

The willingness to approve seizures of equipment in many cases may owe in part to the fact that many of the existing cases involve computers used to store child pornography or, more rarely, obscenity. In such a case, the computer hardware itself technically is an instrumentality of crime and forfeitable.[31] As a result, seizure of the contraband equipment is legal even if some of the files contained in the equipment do not relate to the crime. The Tenth Circuit made this point explicitly

---

[29] Id. at 535 (citations omitted).

[30] Id.

[31] See DOJ MANUAL, supra note 16, at 206.

in the case of *Davis v. Gracey*, which involved a warrant to seize equipment that contained obscenity.[32] The police seized two computer servers used to provide e-mail and digital images to about two thousand subscribers.[33] After the equipment was seized, its owners brought a civil action claiming that the seizure violated the Fourth Amendment.[34] In particular, the plaintiffs claimed that the seizure was overbroad because it seized a great deal of innocent material.[35] The court rejected this argument because the equipment was contraband that could be seized:

> In the typical case, the probable cause supporting seizure of a container is probable cause to believe that the container's contents include contraband or evidentiary material. Here, in contrast, the probable cause supporting the seizure of the computer/container related to the function of the computer equipment in distributing and displaying pornographic images, not to its function in holding the stored files. The fact that a given object may be used for multiple purposes, one licit and one illicit, does not invalidate the seizure of the object when supported by probable cause and a valid warrant.[36]

Even in *Gracey*, however, the court was influenced by the practical difficulties inherent in a contrary rule requiring the police to distinguish between the seizure of computer equipment and the seizure of individual files stored inside. The court explained:

> We . . . note the obvious difficulties attendant in separating the contents of electronic storage from the computer hardware during the course of a search. Perhaps cognizant of the potential burdens of equipment, expertise, and time required to access, copy, or remove stored computer files, plaintiffs have not suggested any workable rule. In short, we

---

32 111 F.3d 1472, 1475-76 (10th Cir. 1997).

33 Id.

34 Id. at 1476.

35 Id.

36 Id. at 1480.

> can find no legal or practical basis for requiring officers to avoid seizing a computer's contents in order to preserve the legality of the seizure of the computer hardware.
>
> . . . Even in the typical case, seizure of a container need not be supported by probable cause to believe that all of the contents of the container are contraband. The seizure of a container is not invalidated by the probability that some part of its "innocent" contents will be temporarily detained without independent probable cause. We will not hold unlawful the otherwise constitutional seizure of the computer equipment in order to prevent the temporary deprivation of plaintiffs' rights to the contents.[37]

In some cases, however, warrants that listed only the physical property seized during the physical search have been found inadequate because they failed to provide sufficient guidance to regulate the search at the electronic stage. The most important example is *United States v. Riccardi*.[38] In *Riccardi*, the police executed a warrant to seize material relating to child pornography from the defendant's home.[39] During the initial search, they saw that the defendant had a computer.[40] The agents applied for a second warrant to allow them to go back and seize the target's computer.[41] The second warrant listed the items to be seized as the target's computer,

> and all electronic and magnetic media stored therein, together with all storage devises [sic], internal or external to the computer or computer system, including but not limited to floppy disks, diskettes, hard disks, magnetic tapes, removable media drives, optical media such as CD-ROM, printers, modems, and any other electronic or magnetic devises used as a peripheral to the computer or computer system, and all electronic media stored within such

---

37 Id. at 1480-81 (citations omitted).

38 405 F.3d 852 (10th Cir. 2005).

39 Id. at 858.

40 Id.

41 Id.

devises.[42]

The warrant did not explain that it was limited to computers used to store child pornography.[43] In an opinion by Judge McConnell, the court held that the warrant was insufficiently particular because it failed to give the police sufficient guidance as to what kind of evidence they could search for during the forensic analysis.[44] "By its terms, the warrant thus permitted the officers to search for anything—from child pornography to tax returns to private correspondence. It seemed to authorize precisely the kind of `wide-ranging exploratory search[] that the Framers intended to prohibit.'"[45] If the warrant had explained the type of evidence that the police were looking for, McConnell suggested, then it would have been sufficiently particular.[46] The inclusion of the type of evidence was not necessary at the initial physical stage because the police could not know which computers actually did store the evidence sought, but was needed at the second electronic stage to limit the search that the forensic specialists conducted.

United States v. Hunter[47] is somewhat similar. In *Hunter*, investigators searched an attorney's office for evidence that he had helped a client launder money.[48] The warrant authorized the seizure of "[a]ll computers . . . [a]ll computer storage devices . . . [and a]ll computer software systems."[49] The district judge found that this description was overbroad because it did not mention "the specific crimes for which the equipment was sought" or incorporate by reference the affidavit's discussion of

---

42 Id. at 862.

43 Id.

44 Id. at 863.

45 Id. at 863 (alteration in quoted text) (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987)). The court admitted the evidence, however, on the ground that it satisfied the good faith standard. Id. at 864.

46 Id. at 863.

47 13 F. Supp. 2d 574.

48 Id. at 578.

49 Id. at 584 (citation omitted).

the search strategy that investigators planned to use in order to avoid interfering with innocuous files protected by the attorney-client privilege.[50] Without this information, the court suggested, the warrant did not provide sufficient guidance to the officers.[51] As in *Ricardi*, however, the court did not suppress the evidence on the ground that the overall care that the officers showed in planning and conducting the search made the "good faith" exception applicable.[52]

Another notable case rejecting a computer warrant as insufficiently particular is a civil decision, *Arkansas Chronicle v. Easley*.[53] In *Easley*, state investigators obtained a warrant to search a journalist's home for evidence relating to the Oklahoma City bombings.[54] The investigators sought a video and three still photographs believed to be located on the journalist's computer.[55] Instead of describing the property to be seized as the video and the photographs, the warrant focused only on the physical stage of the search: the warrant permitted the agents to seize "[a]ny and all computer equipment, hard disk drives, compact disks, floppy disks, magnetic tapes or other magnetic or optical media capable of storing information in an electronic, magnetic or optical format."[56] As in *Riccardi*, the warrant was held invalid on the ground that it did not limit the scope of the electronic search: "In these circumstances, such a warrant essentially amounted to a general warrant giving police the authority to rummage through every single computer file and document with no limitations on which documents could be

---

50 Id.; see also United States v. Clough, 46 F. Supp. 2d 84, 87 (D. Me. 2003) (finding computer warrant unconstitutionally broad when it permitted the seizure of "text documents of any variety, including e-mail, websites, records of chat sessions, correspondence or shipping records; and . . . digital images of any variety, including still images and videos" without additional limitation) (citation omitted).

51 Hunter, 13 F. Supp. 2d at 584.

52 Id. at 584-85.

53 321 F. Supp. 2d 776 (E.D. Va. 2004) (Ellis, J.).

54 Id. at 778.

55 Id. at 793.

56 Id. at 792.

seized."[57] Judge Ellis also expressed concern that the warrant was too broad in terms of limiting the seizure at the initial physical stage, a problem made more severe by the fact that the role of the computer in the case was mere evidence rather than contraband or an instrumentality of crime.[58]

Warrants that list the evidence to be seized as the information sought are less common than warrants that list the evidence to be seized as the physical storage device. Nonetheless, warrants in such cases have been upheld as well.[59] In these cases, the defense challenge generally shifts ground: instead of arguing that the warrant was overbroad, defendants claim that the execution of the warrant was in "flagrant disregard" of the warrant.[60] The "flagrant disregard" standard has been adopted by the courts of appeal to review the execution of a warrant;[61] if the evidence in question was within the scope of the warrant, that evidence is suppressed only if the search so grossly exceeds the scope of the warrant during execution that the authorized search appears to be merely a pretext for a "fishing expedition" through the target's private property.

This is a very difficult standard for defendants to satisfy, as it amounts to a requirement of large-scale bad faith. Proving bad faith is difficult in light of the significant body of caselaw in recent years emphasizing the practical reasons investigators may need to seize computers and subject them to an off-site search. Searching on-site for the evidence can be more disruptive than searching on-site; courts have found it "obvious" that searching a computer for evidence requires great skill, time and

---

[57] Id. at 793 (citation omitted).

[58] Id.

[59] See, e.g., United States v. Gawrysiak, 972 F. Supp. 853, 866-67 (D.N.J. 1997).

[60] See, e.g., United States v. Liu, 239 F.3d 138, 140 (2d Cir. 2000); United States v. Foster, 100 F.3d 846, 849 (10th Cir. 1996); Gawrysiak, 972 F. Supp. at 864.

[61] See, e.g., Liu, 239 F.3d at 140; Foster, 100 F.3d at 851; United States v. Young, 877 F.2d 1099, 1105-06 (1st Cir. 1989). Notably, the Supreme Court has not addressed this issue directly.

expertise.[62] In light of that it is generally more reasonable to allow officers to search off-site than park at the suspect's home for a few days while the search of his computer occurs.[63] As one district judge noted, "[t]he Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant."[64] These precedents make it difficult to establish that a routine computer search was in "flagrant disregard" of the warrant.

The judicial focus on practical reasons why a warrant must be executed in a particular way has led to a new practice among prosecutors and law enforcement agents in the case of digital evidence searches. In traditional cases, the affidavit in support of the warrant explains the officer's probable cause to believe that evidence described in the warrant will be located in the place searched. In digital evidence warrants the affidavit is used to do much more. In many cases, the affidavit is used to explain the need for a two-step search to the magistrate judge. The affidavit informs the judge of what investigators plan to do when they execute the warrant, explaining the practical needs that they believe justify the two-step search process. The magistrate's decision to sign the warrant in effect "approves" the two-stage search ex ante.[65] With the search process approved before the search is executed, a defendant will have a hard time arguing that the search was executed in "flagrant

---

[62] Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (noting "the obvious difficulties attendant in separating the contents of electronic storage [sought as evidence] from the computer hardware [seized] during the course of a search.").

[63] United States v. Henson, 848 F.2d 1374, 1383-84 (6th Cir. 1988) ("We do not think it is reasonable to have required the officers to sift through the large mass of documents and computer files found in the [defendant's] office, in an effort to segregate those few papers that were outside the warrant.") (citation omitted).

[64] Gawrysiak, 972 F. Supp. at 866.

[65] Cf. United States v. Hay, 231 F.3d 630, 634 (9th Cir. 2000) (upholding magistrate's authorization to both seize and search a computer).

disregard" of the warrant or that it was overbroad.

The idea of justifying the overbroad seizure through language in the affidavit derives in part from an early Ninth Circuit case involving paper documents, *United States v. Tamura*.[66] In *Tamura*, the government seized boxes of documents and took them offsite for review. The boxes contained some documents which were evidence of crime commingled with innocuous documents, and the government seized all of them because of the infeasibility to search through all boxes on site.[67] In an opinion by Judge Fletcher, the Ninth Circuit offered a suggestion for how the government could "generally . . . avoid violating [F]ourth [A]mendment rights" in cases involving commingled documents: get prior permission to seize all of the documents and conduct an off-site search before actually doing so, in order that "wholesale removal" is "monitored by the judgment of a neutral, detached magistrate."[68] In other words, judges should sign off on the wholesale seizure of documents so overbroad seizures are not conducted unless they are required by practical concerns.[69]

The Justice Department has recommended something akin to the *Tamura* approach in its manual on *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.[70] The DOJ Manual recommends the following practice when the physical storage device is only a storage container for evidence:

> The affidavit should . . . contain a careful explanation of the agents' search strategy, as well as a discussion of any practical or legal concerns that govern how the search will be executed. Such an explanation is particularly important

---

66 694 F.2d 591, 594-95 (9th Cir. 1982).

67 Id. at 595.

68 Id. at 595-96.

69 Id. at 596.

70 DOJ MANUAL, supra note 16, at 70, 72. In the interest of full disclosure, I should note that I wrote this manual under the auspices and with the guidance of others at the Department of Justice.

> when practical considerations may require that agents seize computer hardware and search it off-site when that hardware is only a storage device for evidence of crime. Similarly, searches for computer evidence in sensitive environments (such as functioning businesses) may require that the agents adopt an incremental approach designed to minimize the intrusiveness of the search. The affidavit should explain the agents' approach in sufficient detail that the explanation provides a useful guide for the search team and any reviewing court. It is a good practice to include a copy of the search strategy as an attachment to the warrant, especially when the affidavit is placed under seal.[71]

Exactly what kind of detail is required in the affidavit presently remains an open question. As I explain in another article, a few courts have indicated that the search strategy should include the specific steps that will be undertaken when the forensic analyst conducts the electronic search.[72] That is, the affidavit should not only explain the need for a two-stage search, but should actually provide a detailed list of the steps that will be taken during the second stage. As I argue elsewhere, it is my view that such detail should not be required, especially ex ante, and that the reasonableness of the electronic search should be reviewed ex post using the same "flagrant disregard" standard used in physical searches.[73] But the present uncertainty of how much detail an affidavit should include does not alter the broad acceptance of the basic strategy: prosecutors can "cure" any defect caused by the two-stage warrant process by explaining the process in the affidavit. By signing the warrant, the judge in effect approves the two-stage search and cures what otherwise would be a technical defect raised by trying to force a two-stage process into a legal rule designed to handle a single-stage search.

---

71 Id. at 219.

72 Kerr, supra note 8.

73 Id.

B. When Can the Search be Executed?

The last five years have witnessed a considerable amount of litigation—not to mention a great deal of informal negotiations between prosecutors and magistrate judges—on when a search for digital evidence can be executed. The legal issues fall into two basic categories. The first set of issues concerns whether the timing restrictions of warrant rules such as Rule 41 apply to the subsequent electronic search. The second set of issues concerns the legality and propriety of judicially-imposed restrictions on the timing of the electronic search process. The first questions have a reasonably clear answer. The second do not.

The few courts that have addressed the first issue have held that statutory rules requiring the search to occur within a particular time window do not apply to the computer forensic process. For example, in *Commonwealth v Ellis*,[74] investigators seized a computer server at a law firm.[75] The defendant relied on a state supreme court decision that had interpreted the state warrant law to require that every search pursuant to a warrant must be completed within seven days of the warrant being issued. The *Ellis* court concluded that this did not apply to the computer forensic process.[76] According to the Court:

> [the state supreme court's interpretation of state law] was made before the advent of the computer age, and before the Supreme Judicial Court could envision a scenario where execution of a search could continue after the return of the warrant had been filed. And where computers are seized, that is precisely what occurs. . . . Courts have recognized that the search of computer data involves more preparation than an ordinary search and a greater degree of care in the

---

[74] 10 Mass. L. Rptr. 464, 1999 Mass. Super. LEXIS 368 (Mass. Super. Ct. 1999).

[75] Id.

[76] Id.

> execution of the warrant; and that the search may involve much more information. As such, computer searches are not, and cannot be, subject to the statutory requirement that the search be completed within seven days.[77]

Federal courts have reached the same conclusion in the context of interpreting the ten-day rule of Rule 41, which requires warrants to be executed within ten days of being signed. A handful of federal district courts have addressed the issue and held that the computer forensic process is not included within the ten day rule.[78] As one court explained in *United States v. Hernandez*:

> Neither Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant. In most cases the forensic examination of the computer will take place at a different location than that where the computer was seized. The same principle applies when a search warrant is performed for documents. 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. The examination of these items at a later date does not make the evidence suppressible.[79]

The more difficult questions concern the second set of issues.

---

[77] Id. at *29-*30 (footnote and citations omitted).

[78] United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) ("The warrant did not limit the amount of time in which the government was required to complete its off-site forensic analysis of the seized items and the courts have not imposed such a prophylactic constraint on law enforcement."); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (stating that Rule 41 does not "provide[] for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant."); United States v. Crim. Triumph Capital Group, 211 F.R.D. 31, 66 (D. Conn. 2002); United States v. Habershaw, 2001 WL 1867803, at *8 (D. Mass. May 13, 2001).

[79] Hernandez, 183 F. Supp. 2d at 480.

First, are there any constitutional limits on when the electronic search must occur? Second, do magistrate judges have the statutory authority to condition the issuance of the warrant on the government's agreement to conduct the electronic search in a particular period of time? Two federal district courts have recently suggested that the Fourth Amendment's reasonableness standard requires the investigators to search the computer for the evidence before too much time has elapsed. The apparent idea is that an excessive delay before the second search renders the continued seizure unreasonable, requiring suppression of the evidence as fruit of an unreasonable seizure.[80]

The first of the two cases is *United States v. Grimmett*.[81] In *Grimmett*, officers seized computers pursuant to a state warrant that authorized a search for child pornography.[82] State law gave the officers ninety-six hours to execute the search.[83] The officers seized the computers from the defendant's home within the ninety-six-hour window, but then a few weeks passed before the government's computer expert searched the computer for child pornography.[84] The defendant claimed that the failure to search the computer for evidence within the ninety-six-hour window violated the Fourth Amendment.[85] The court rejected the claim, but did accept the basic idea that the timing of the computer search was governed by a reasonableness analysis:

> The conduct of law enforcement officers in executing a search warrant is governed by the Fourth Amendment's mandate of reasonableness. The Fourth Amendment does not provide a specific time in which a computer may be subjected to a government forensic examination after it has been seized pursuant to a search warrant. The court finds that the Fourth Amendment requires only that the subsequent search of the computer be made within a reasonable

80 See Ellis, 10 Mass. L. Rptr. at *29.

81 2004 WL 3171788 (D. Kan. 2005).

82 Id. at *1-*2.

83 Id. at *1.

84 Id. at *2.

85 Id. at *3.

> time . . . . The court finds that the subsequent search was conducted within a reasonable time since it was concluded within a few weeks of the execution of the warrant.[86]

The second case is *United States v. Syphers*.[87] The *Syphers* court held that a seven month delay in the forensic analysis of a computer was reasonable because it was justified by legitimate practical needs:

> Syphers asserts that the state acted unreasonably in detaining the CPU for seven months before completing the search. The government counters that the Fourth Amendment does not impose any limitation on the length of a forensic examination of a computer. "However, from the general prohibition against `unreasonable searches and seizures' . . . it may be contended that there are some constitutional limitations upon the time when a search warrant may be executed." . . .
>
> Based on the same reasons which support the finding that the state acted in good faith with respect to the warrant, the court concludes that the state did not overstep any constitutional boundaries in seizing the CPU for seven months under the circumstances presented.[88]

The *Syphers* court then cited a military court decision by the U.S. Navy-Marine Corps Court of Criminal Appeals in *United States v. Greene*.[89] In *Greene*, Special Agents of the Naval Criminal Investigatory Service (NCIS) obtained the target's consent to seize and search the suspect's computer for child pornography.[90] The consent form did not state the length of time that Greene agreed to allow the NCIS to seize his computer,

---

86 Id. at *5 (citation omitted).

87 296 F. Supp. 2d 50 (D.N.H. 2003), aff'd, 2005 U.S. App. LEXIS 22527 (1st Cir. 2005) (the First Circuit affirmed, but relied on circuit precedent that did not directly address reasonableness).

88 Id. at 59 (citation omitted).

89 56 M.J. 817 (N-M. Ct. Crim. App. 2002).

90 Id. at 820.

but three months elapsed before the forensic process was undertaken.[91] The court concluded that the three month delay was not unreasonable:

> While the appellee did not expressly consent to a period of 3 months of NCIS seizure and retention of his property, the plain language of the consent form clearly states he agreed to allow the investigators to remove and retain his property for investigative purposes. In other words, the appellee consented to a seizure of his property. If the appellee believed that retention for 3 months was unreasonable, he never said so. We hold that, in this case, the consensual seizure and subsequent retention for 3 months was not unreasonable.[92]

In a footnote, however, the court warned that there were limits to when the search could be completed:

> Although we hold that 3 months is constitutionally permissible here, we also believe that an excessively long period of retention, following a lawful seizure, could be unreasonable. We decline to try to draw a "bright-line" that would apply in all circumstances. Each case must be considered on its own facts.[93]

While *Grimmett*, *Syphers* and *Greene* suggest that an excessive delay in the forensic process may render the seizure unreasonable, it is unclear whether this suggestion makes sense in light of existing law. First, the computers in all three cases were instrumentalities of the crime: they were used to possess illegal images of child pornography. Given that these items are forfeitable, it makes little sense to suggest that continued deprivation of the property renders the seizure unreasonable. Second, statements by prior courts and commentators that delay in the timing of a search may have constitutional

---

91 Id. at 821-23.

92 Id. at 823.

93 Id. at n.4.

limitations were made in the context of an initial physical search. In those circumstances, delay may allow the probable cause to become stale. The search is unreasonable because as time passes the case for probable cause begins to evaporate. In contrast, a seized computer stores its information permanently. The initial physical search and seizure has already occurred. The cause can no longer become stale.

Whether the framework suggested in *Grimmett*, *Syphers* and *Greene* will be adopted by other courts remains unclear. A large body of case law indicates that the amount of time that property or a person is seized factors into the reasonableness of the seizure.[94] Courts could therefore hold that a warrant authorizes a theoretically overbroad computer seizure, but that as time passes the overbroad seizure becomes less reasonable. One difficulty with this approach is that the vague standard gives little guidance to law enforcement. Most agents and prosecutors are at the mercy of forensic lab employees with regard to the timing of the electronic search. The timing of a search may be determined by the lab's resources, the forensic analyst's skills, the specific tools the lab uses, and the type of investigation. A general reasonableness requirement does not provide clear guidance to law enforcement and may end up punishing agents and prosecutors for factors beyond their control. A better approach would be to provide clear guidance using statutory warrant rules.

A related issue is whether magistrate judges have the statutory authority to condition the issuance of a warrant on the government's agreement to search the computers, or at least begin the search, within a specific period of time. As the DOJ Manual explains:

> Several magistrate 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. Some magistrate judges have imposed time limits as short as seven days, and

[94] See, e.g., United States v. Place, 462 U.S. 696, 703 (1983).

> several have imposed specific time limits when agents apply for a warrant to seize computers from operating businesses. In support of these limitations, a few magistrate judges have expressed their concern that it might be constitutionally "unreasonable" under the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time.[95]

Do magistrate judges have the power to do this? The text of Rule 41 is not entirely clear, but suggests that judges may not. Rule 41(d)(1) is phrased as a command: "a magistrate judge . . . *must* issue the warrant if there is probable cause."[96] The rule appears to give the judge no power to withhold the warrant unless the government agrees to a special condition. As the DOJ Manual explains:

> the relevant case law is sparse, [but] it suggests that magistrate judges lack the legal authority to refuse to issue search warrants on the ground that they believe that the agents may, in the future, execute the warrants in an unconstitutional fashion. See Abraham S. Goldstein, The Search Warrant, the Magistrate, and Judicial Review, 62 N.Y.U. L. REV. 1173, 1196 (1987) ("The few cases on [whether a magistrate judge can refuse to issue a warrant on the ground that the search may be executed unconstitutionally] hold that a judge has a `ministerial' duty to issue a warrant after `probable cause' has been established."); In re Worksite Inspection of Quality Prod., Inc., 592 F.2d 611, 613 (1st Cir. 1979) (noting thel imited role of magistrate judges in issuing search warrants). As the Supreme Court suggested in one early case, the proper course is for the magistrate to issue the warrant so long as probable cause exists, and then to permit the parties to litigate the constitutional issues afterwards. See Ex Parte United States, 287 U.S. 241, 250 (1932) ("The refusal of the trial court to issue a warrant . . . is, in reality and effect, a refusal to permit the case to come to a hearing upone ither questions of

---

95 DOJ MANUAL, supra note 16, at 77.

96 FED. R. CRIM. P. 41(d)(1) (emphasis added).

> law or fact and falls little short of a refusal to permit the enforcement of the law.").[97]

There are other perspectives, however. Susan Brenner and Barbara Frederiksen have argued that Rule 41 creates a "reservoir of inherent power" to place time restrictions on the computer forensic process.[98] They note that courts have allowed federal judges to issue anticipatory warrants that are triggered when some future event happens.[99] For example, the police can obtain a warrant to search a house the moment a suspicious package is delivered and can condition the execution of the warrant on the arrival of the suspicious package at the location to be searched. Brenner and Frederiksen suggest that restrictions on the timing of the computer forensic process are similar and thus implicitly allowed by Rule 41.[100]

I am not sure I am convinced by this argument. Anticipatory warrants are generally justified by the timing of probable cause. The thinking is that probable cause to execute the search is contingent on the condition precedent, such as the arrival of the package, occurring.[101] The warrant can be executed only when the condition precedent occurs because until that point, no probable cause exists and no warrant can issue unless probable cause exists. Further, Rule 41 has been amended specifically to allow for anticipatory warrants.[102] In light of

---

97 DOJ MANUAL, supra note 16, at 77-78.

98 Brenner & Frederiksen, supra note 4, at 114.

99 Id.

100 Id.

101 See, e.g., United States v. Grubbs, 377 F.3d 1072, 1077-78 (9th Cir.), reh'g denied, 389 F.3d 1306 (9th Cir. 2004), cert. granted, 74 U.S.L.W. 3199 (U.S. Sept. 27, 2005).

102 United States v. Tagbering, 985 F.2d 946, 949 n.3 (8th Cir. 1993) (noting that a 1990 amendment to Rule 41(a)(1) "permits anticipatory warrants" (quoting FED. R. CRIM. P. 41 advisory committee's note (1990 amendments))); see also FED. R. CRIM. P. 41(b)(2) ("[A] magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might

these differences, I do not see how the power to issue anticipatory warrants implies the power to control the timing of the computer forensic process. Making a police officer wait to execute a warrant until there is probable cause seems quite different from making an officer conduct a forensic analysis of a seized computer within a specific window of time. In any event, the magistrate's power to impose time limits on the forensic process presently remains unclear.[103]

As a practical matter, agents will have little choice but to follow time limits on the forensic process when judges decide to impose them. In *United States v. Brunette*,[104] a magistrate judge allowed agents to seize the computers of a child pornography suspect, but added the condition that the forensic analysis must occur "within 30 days."[105] The agents seized two computers when they executed the search five days later.[106] A few days before the thirty-day period elapsed, agents obtained a thirty-day extension for review.[107] They examined one of the seized computers within the thirty-day extension period and found pornographic images of children.[108] However, the agents did not begin the review of the last computer until shortly after the extension period had elapsed.[109] Brunette argued that the evidence located on the last computer had to be suppressed because the search outside of the sixty-day period violated the terms of the judge's order.[110] The district court agreed, conclud-

move or be moved outside the district before the warrant is executed").

[103] See also West End, 321 F. Supp. 2d at 961 (holding that the magistrate has the power to require the submission of search protocol to fulfill the requirements of particularity and probable cause before a computer can be searched pursuant to a warrant).

[104] 76 F. Supp. 2d 30 (D. Me. 1999), aff'd, 256 F.3d 14 (1st Cir. 2001).

[105] Id.

[106] Id.

[107] Id.

[108] Brunette, 256 F.3d at 16.

[109] Brunette, 76 F. Supp. 2d at 42.

[110] Id.

ing that the failure "to adhere to the requirements of the search warrant and subsequent order" meant that "any evidence gathered from the . . . computer is suppressed."[111]

C. What Are the Oversight and Record-keeping Requirements, and When Must Property be Returned?

Finally, a few courts have touched on the record-keeping requirements of statutory warrant rules and the return of seized computers. The thrust of the caselaw on record-keeping requirements is that they do not apply to the data. For example, the return on the warrant is limited to the physical property taken.[112] The federal rule requires notice, but that notice need only be of the "property taken," which presumably applies only to the physical equipment.[113] This is a sensible approach. The purpose of leaving a return is to inform the suspect of what property was taken, and this is best done by leaving a report of the physical property seized. After all, the suspect himself will know better than the police what files the storage device contains. It does not serve any interest of the warrant rules to require the police to search the computer, catalog its contents, and then notify the ower of what data resides on his hard drive.

The caselaw on the return of physical property treats computers essentially like any other property. The basic rule is that if the government has a continuing need for the property, it can continue to hold it. As the DOJ Manual explains, this standard allows the government to hold on to seized computers throughout the forensic process:

> Rule 41(e) motions requesting the return of properly seized computer equipment succeed only rarely. First, courts will usually decline to exercise jurisdiction over the

---

111 Id.

112 See Ellis, 10 Mass. L. Rptr. at *9 (holding that the search of the files stored on the computer did not have to be finished within the time period required for return of the warrant).

113 United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000).

> motion if the government has offered the property owner an electronic copy of the seized computer files.
>
> Second, courts that reach the merits generally find that the government's interest in the computer equipment outweighs the defendant's so long as a criminal prosecution or forfeiture proceeding is in the works. If the government does not plan to use the computers in further proceedings, however, the computer equipment must be returned. Further, a court may grant a Rule 41(e) motion if the defendant cannot operate his business without the seized computer equipment and the government can work equally well from a copy of the seized files.[114]

Notably, the current rule does not provide any mechanism to allow a suspect to get a copy of seized files unrelated to the investigation. While investigators may decide to generate copies of particular files on their own for suspects, no legal rule requires it.[115]

IV. RETHINKING THE WARRANT PROCESS IN AN AGE OF DIGITAL EVIDENCE

What is the future of the warrant process? This section proposes a series of changes to the law governing the warrant process to update it for the era of digital evidence. It focuses specifically on changes to statutory warrant rules and, in particular, to Rule 41. The goal is to envision how Rule 41 and equivalent state rules might be changed to respond to the specific issues raised by the switch from physical evidence to digital evidence.

Before beginning, it may be helpful to understand why this section focuses on statutory warrant rules rather than the

---

[114] DOJ MANUAL, supra note 16, at 81 (citations omitted).

[115] Id. The DOJ Manual recommends that agents should return "innocent files" to suspects if the suspects can show a "legitimate need" for the files or hardware and the agents can return the files "without either jeopardizing the investigation or imposing prohibitive costs on the government." Id. at 77 n.13.

Fourth Amendment. The primary reason is that Fourth Amendment warrant rules are far more flexible than statutory commands. As the Supreme Court has stressed,

> the Fourth Amendment's commands, like all constitutional requirements, are practical and not abstract. If the teachings of the Court's cases are to be followed and the constitutional policy served, affidavits for search warrants, such as the one involved here, must be tested and interpreted by magistrates and courts in a commonsense and realistic fashion. They are normally drafted by nonlawyers in the midst and haste of a criminal investigation. Technical requirements of elaborate specificity once exacted under common law pleadings have no proper place in this area. A grudging or negative attitude by reviewing courts toward warrants will tend to discourage police officers from submitting their evidence to a judicial officer before acting. [116]

Courts generally have heeded this guidance on the case of computer searches and seizures. For the most part, judges have proved sensitive to the practical difficulties inherent in computer searches and seizures, and they have not imposed highly restrictive requirements that would not work for the two-step warrant process.[117] Given the presumption that searches pursuant to warrants are constitutionally reasonable, courts have generally approved two-stage searches within the reasonableness framework of the Fourth Amendment.

Statutory warrant rules are less flexible and more detailed, and therefore play a greater role in light of changing facts. Statutory warrant rules such as Rule 41 are designed to regulate the traditional physical search process. They are poorly equipped to fit the two-stage search warrant process needed in the case of most computer searches and seizures. The rules remain rigid and specific, and are therefore less able to accommodate the dynamics of digital evidence searches. As a result,

---

116 United States v. Ventresca, 380 U.S. 102, 108 (1965).

117 See supra notes 27-64 and accompanying text.

legal reform must focus on statutory warrant rules. Of course, constitutional and statutory rules have a symbiotic relationship. A revision of existing statutory warrant rules can help address the Fourth Amendment's reasonableness command. New statutory rules that better regulate the warrant process can permit a better fit between the new facts and the animating concerns of Fourth Amendment law.

A. The Thing to be Seized

The first change I propose is modifying Rule 41's current requirement that "[t]he warrant must identify the person or property to be searched, [and] identify any person or property to be seized."[118] In digital evidence cases, more specific language should be used. The language should require the police to state what physical evidence they plan to seize on-site, and then indicate what kind of evidence they plan to search for in the subsequent electronic search. In other words, agents should be required to describe the property to be seized at *both* the physical search stage *and* the electronic search stage.

This could be achieved by amending Rule 41(e) to add an additional sentence. Something like this should work:

> If the the warrant authorizes the seizure of computers or electronic storage devices to retrieve computer data constituting evidence of crime, the warrant must identify both the physical computers or storage devices to be seized and the computer data that constitutes evidence of the crime.

Under this approach, a computer warrant would require the officers to name the specific evidence they are searching for twice, correlating with the two stages of criminal investigations. For example, the warrant form could authorize the police to seize "all computers and electronic storage devices believed to contain evidence of wire fraud" while on-site and then authorize

[118] FED R. CRIM. P. 41(e)(2).

a subsequent search for the specific files that the agents have reason to believe are located on the storage device. This approach would address both the particularity concern and also ensure that the warrant is not executed in disregard of the warrant.

A second and related change should be made to Rule 41(b) and (d) to make clear that searches to retrieve information but not seize physical property are permissible. The current text of Rule 41 states that a warrant can be issued "to search for and seize a person or property located within the district."[119] When computer information is copied, however, no seizure occurs; the owner is not actually deprived of his property.[120] It is well-settled that Rule 41 can be used to obtain a warrant for mere information; this was the apparent holding of *United States v. New York Telephone Co.*,[121] and was reaffirmed in early cases holding that a Rule 41 warrant could be obtained to collect computer data.[122] However, this interpretation was reached through the meaning of "property" in Rule 41,[123] apparently without recognition that copying data does not seize it. In light of the meaning of seizure in the context of electronic evidence, it may be appropriate to modify Rule 41 formally to note that a seizure is not a prerequisite of a search.

---

119 Id. at 41(b)(1).

120 See Kerr, supra note 3, at 301.

121 434 U.S. 159, 170 (1977).

122 See, e.g., United States v. Hall, 583 F. Supp. 717, 718-19 (E.D. Va. 1984).

123 See United States v. N.Y. Tel., 434 U.S. 159, 170 (1977).

B. The Place to be Searched

Statutory warrant rules could also be amended to consider the case of computers in government custody. Alternatively, courts could simply approve warrants that describe the place to be searched in such cases as the computer itself. For example, imagine an FBI field office has a computer in its possession and needs a search warrant to search the machine. The "place to be searched" could be a particular description of the computer itself, held in the custody of the FBI field office. That is, the warrant would name the specific movable property to be searched, rather than the physical place where that movable property happens to be stored.

C. When Can the Search be Executed?

Significant changes should be made to Rule 41 and equivalent state provisions to specify when each stage of the two-step warrant process must be executed. Rule 41(e)(2) states that a federal search warrant "must command the officer to: (A) execute the warrant within a specified time no longer than 10 days; (B) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time."[124] One obvious change would be to amend this language to clarify that the ten-day and daytime rules do not apply to the subsequent electronic search, as the *Hernandez* court concluded.[125] Perhaps the easiest way to do this would be to include a definition of "execute the warrant" in the case of computer searches. For example, the following addition to the definition section of the Rule 41(a)(2) could do the trick:

> In a case involving the seizure of computers and other electronic storage devices, the execution of the warrant refers

[124] FED. R. CRIM. P. 41(e)(2).

[125] *Hernandez*, 183 F. Supp. 2d at 480-81.

> to the seizing of the computers and storage devices rather than any subsequent search of their contents.

Rule 41 also should be amended to add clear guidance on when a computer must be searched and when it should be returned. Instead of leaving this to individual magistrate judges, a uniform standard should be used. The standard should consider two important practical points. First, backlogs and delays at government forensic laboratories are common, and they are almost always beyond the control of the individual agent or prosecutor who obtains the warrant. While we might hope that the relevant legislature funds such labs properly and they can be staffed competently, it would be inappropriate to punish agents if the forensic experts have a backlog and cannot search equipment quickly. Second, when a computer device is seized only for the evidence it contains, and is not itself contraband, a fruit, or an instrumentality of crime, the government's interest in the property can be satisfied by generating a bitstream copy of the storage device. It is relatively quick and easy for a government forensic analyst to generate a bitstream copy of the storage device. Indeed, it is a necessary first step of every forensic analysis: a computer normally is searched by generating a copy of its data, and then searching the copy instead of the original.[126] In cases where the computer is used only as a storage device, the computer itself can be returned after the government has generated the bitstream copy.

In light of these practical concerns, my proposal would be to create two distinct rules to govern the timing of the forensic process. In cases where the computer is merely a storage device for evidence, the government should be required to seize the computer, create a bitstream copy of its files, and then return the property to its proper owner in a reasonable period of time, such as thirty days. The agents should be allowed to request an extension of this time period for additional thirty-day periods for good cause; this may be necessary because some computers

[126] See Kerr, supra note 8.

may prove difficult to image. In addition, the rule could include provisos about ensuring that copies are recognzied to be equivalent to the original. For example, one option would be to give the defendant access to the copy and conditioning return of the computer on the defendant's stipulation that the copy is accurate. I am not sure such a provision is necessary, as investigators need to establish the reliability of computer copies in any event. At the same time, such a provision could ensure that the need to return property to a suspect does not fuel defense challenges to the accuracy of the government's copy that would be avoided in cases where the government can keep the original computer hardware.[127]

Requiring investigators to copy the data and returning the equipment in thirty days would also address possible constitutional problems without imposing a terrible burden on investigators. *Syphers* and *Greene* suggest that retaining a target's computer hardware for an excessive period of time may eventually render the seizure unreasonable, even pursuant to a warrant.[128] A thirty-day rule could address this concern by forcing government action and return of the computer before the seizure becomes unreasonable.

When the computer hardware is believed to be a fruit, instrumentality of crime, or contraband, the warrant should contain a different set of requirements. In these cases, the key question is whether the physical computer storage device already seized *actually is* a fruit, instrumentality of crime, or contraband. Agents generally find this out by beginning the electronic search and identifying material such as child pornog-

[127] Susan Brenner and Barbara Frederiksen offer a somewhat similar proposal, focused on ensuring that targets have copies of seized files rather than hardware:

> When a court issues a seizure and an off-site search authorization, it should require that the officers create at least one back-up copy of the information on the seized equipment and give this back-up copy to the owner of that equipment.

Brenner & Frederiksen, supra note 4, at 79.

[128] Syphers, 296 F. Supp. 2d 50; Greene, 56 M.J. at 817.

raphy or hacking evidence. If the material is discovered on the computer, then the person from whom the property was taken has no legal right to the property; it need not be returned, and in fact will likely support legal forfeiture proceedings. In light of this, Rule 41 should require investigators to begin the forensic process and establish whether the computer contains at least some of the relevant material within a particular period of time, such as sixty days.[129] If agents locate the evidence on the computer, then they do not need to return it. However, if they cannot find any evidence showing that the computer itself is a fruit, instrumentality, or contraband, then agents should be permitted to retain the copy generated during the forensic process but should be required to and return the computer equipment. This would allow investigators to continue their search for evidence if needed, but without depriving the target of his property. As with the first set of rules, agents should be permitted to apply for extensions of time for good cause.

The goal of these rules would be to identify some kind of middle ground that recognizes both the difficulty of the computer forensic process and the competing interests of computer owners. A warrant to seize a computer that has a small amount of incriminating evidence on it should not provide a license for the government to seize the computer indefinitely. Instead, there should be set (if ultimately flexible) standards for when agents must generate copies of files and return the hardware in cases where the physical storage device is not independently seizable. Further, similar standards should be defined for when agents must begin the forensic process and identify whether the computer is independently seizable because the computer is contraband, a fruit, or an instrumentality of crime.

[129] Cf. Brenner & Frederiksen, supra note 4, at 84.

D. What are the Oversight and Record-keeping Requirements, and When Must Property be Returned?

The final issue concerns oversight and record-keeping requirements, as well as the law governing when property should be returned. I think the latter question is best addressed by the rule just discussed on the timing of the forensic process. If the police are generally required to conduct enough of the forensic process at an early enough stage that the computer hardware must either be returned or the status of the property as contraband confirmed, then there is no need for a new rule specifically governing the return of property.

The question of what record-keeping requirements to mandate is difficult to answer at this time because the underlying Fourth Amendment rules remain unclear. As I detail in another article, courts have not settled on a uniform standard for reviewing the computer forensic process.[130] The record-keeping requirements of Rule 41 and analogous state rules should track the developing Fourth Amendment standards; extensive records should be kept if courts closely scrutinize the forensic process under the Fourth Amendment, but not otherwise. Until we know more about what Fourth Amendment standards apply, it is too early to settle on the proper Rule 41 standard.

One rule that does not need to be changed concerns the inventory requirement presently for the return of the warrant. The inventory requirement is presently limited to physical hardware, and in my view it should remain so limited. Susan Brenner and Barbara Frederiksen have taken a different view. They argue that the return on the warrant should include "a detailed inventory of the hardware that is seized and of the data and files that are seized."[131] They write:

> These inventories should be supplied in addition to the back-up copies of any seized data. The inventories are not substi-

---

130 See Kerr, supra note 8.

131 Brenner & Frederiksen, supra note 4, at 80.

> tutes for back-up copies. . . . For computer media or seized files the inventory should describe the type of media, capacity (if known), number seized, and a listing of the files contained on the media. This listing of files should detail, at a minimum, the file name, creation date, access date, file size, and the location of the file on the disk (either the full path of the file, or its absolute address on the disk).[132]

I find this approach problematic. The inventory requirement is designed to facilitate judicial review of the warrant process.[133] The suspect needs to know what was taken if he wishes to challenge the seizure. Accessing computer storage devices and compiling a list of each device's contents does not serve this function. The owner of the computer knows what is on the storage device, and taking the physical device obviously takes all of its contents. Further, such an inventory requirement may have the perverse effect of expanding the government's power to search the computer. Completing the inventory would enable the government to find out all the file names and sizes of the material on the hard drive, which might then provide clues to unrelated crimes. While such steps may or may not be acceptable under the Fourth Amendment, requiring them to be taken as part of Rule 41 allows the inventory task to serve an investigatory function.[134] On balance, I think that an inventory limited to physical storage devices should be sufficient.

---

[132] Id.

[133] See generally South Dakota v. Opperman, 428 U.S. 364, 369-71 (1976).

[134] United States v. Flores, 122 F. Supp. 2d 491, 494-95 (S.D.N.Y. 2000); United States v. O'Razvi, 1998 WL 405048, at *6-7 (S.D.N.Y. July 17, 1998).

CONCLUSION

Law enforcement's increasing need to collect digital evidence raises many challenges for the law of criminal procedure. The shift from physical evidence to digital evidence often leads to a shift in how investigators collect evidence; changes in how evidence is collected leads to pressure for new legal rules to regulate evidence collection. The warrant process is merely one part of a broader mosaic of the mechanisms of the investigative process that will be reformed. It is also a particularly clear example of how technology will require changes in law: computer technologies bifurcate the warrant process from its traditional one-step process to a two-step process, creating a need for legal rules to regulate the second step.

Reforming the warrant process also presents an unusual opportunity for the legal system to experiment with new legal rules in response to the shift to digital evidence. At the federal level, an advisory committee has the power to propose changes to the Federal Rules of Criminal Procedure.[135] In the case of Rule 41, the Rules Committee rather than the courts are best suited to address the problem; Rule 41 issues may occupy the time of judges and prosecutors, but they only rarely lead to litigation that can result in judicial rethinking of the legal standards.[136] The Federal Rules Committee should take the lead in this area and rethink Rule 41 for the era of digital evidence. Changes in Rule 41 can influence similar changes at the state

[135] See 28 U.S.C. §§ 2072-74 (2000). Under federal law, an advisory committee created by the Judicial Conference makes recommendations to the Supreme Court, which then approves or rejects changes pursuant to a Congressional notice provision.

[136] This is true for two reasons. First, a judge's refusal to sign a warrant application is not ordinarily an appealable final order. See United States v. Savides, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987), aff'd in relevant part sub nom.; United States v. Pace, 898 F.2d 1218, 1230 (7th Cir. 1990). Second, violations of Rule 41 rarely lead to suppression of evidence. See generally United States v. Calandra, 414 U.S. 338, 341-42 (1974).

level, and even provide an international standard that will guide other countries facing the same clash between new technologies and existing legal rules.

APPENDIX

Federal Rules of Criminal Procedure 41.
Rule 41. Search and Seizure

(a) Scope and Definitions.

(1) Scope. This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.

(2) Definitions. The following definitions apply under this rule:

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time.

(C) "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorized by the Attorney General to request a search warrant.

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed; and

(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism (as defined in 18 U.S.C. § 2331)—having authority in any district in which activities related to the terrorism may have occurred, may issue a warrant for a person or property within or outside that district.

(c) Persons or Property Subject to Search or Seizure. A warrant may be issued for any of the following:

(1) evidence of a crime;

(2) contraband, fruits of crime, or other items illegally possessed;

(3) property designed for use, intended for use, or used in committing a crime; or

(4) a person to be arrested or a person who is unlawfully restrained.

(d) Obtaining a Warrant.

(1) Probable Cause. After receiving an affidavit or other information, a magistrate judge or a judge of a state court of record must issue the warrant if there is probable cause to search for and seize a person or property under Rule 41(c).

(2) Requesting a Warrant in the Presence of a Judge.

(A) Warrant on an Affidavit. When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

(B) Warrant on Sworn Testimony. The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

(C) Recording Testimony. Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

(3) Requesting a Warrant by Telephonic or Other Means.

(A) In General. A magistrate judge may issue a warrant based on information communicated by telephone or other appropriate means, including facsimile transmission.

(B) Recording Testimony. Upon learning that an applicant is requesting a warrant, a magistrate judge must:

(i) place under oath the applicant and any person on whose testimony the application is based; and

(ii) make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.

(C) Certifying Testimony. The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.

(D) Suppression Limited. Absent a finding of bad faith, evidence obtained from a warrant issued under Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

(e) Issuing the Warrant.

(1) In General. The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it.

(2) Contents of the Warrant. The warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(A) execute the warrant within a specified time no longer than 10 days;

(B) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and

(C) return the warrant to the magistrate judge designated in the warrant.

(3) Warrant by Telephonic or Other Means. If a magistrate judge decides to proceed under Rule 41(d)(3)(A), the following additional procedures apply:

(A) Preparing a Proposed Duplicate Original Warrant. The applicant must prepare a "proposed duplicate original warrant" and must read or otherwise transmit the contents of that document verbatim to the magistrate judge.

(B) Preparing an Original Warrant. The magistrate judge must enter the contents of the proposed duplicate original warrant into an original warrant.

(C) Modifications. The magistrate judge may direct the applicant to modify the proposed duplicate original warrant. In that case, the judge must also modify the original warrant.

(D) Signing the Original Warrant and the Duplicate Original Warrant. Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact time it is issued, and direct the applicant to sign the judge's name on the duplicate original warrant.

(f) Executing and Returning the Warrant.

(1) Noting the Time. The officer executing the warrant must enter on its face the exact date and time it is executed.

(2) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person.

(3) Receipt. The officer executing the warrant must:

(A) give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken; or

(B) leave a copy of the warrant and receipt at the place where the officer took the property.

(4) Return. The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(g) Motion to Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

(h) Motion to Suppress. A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.

(i) Forwarding Papers to the Clerk. The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.