

SEARCHES AND SEIZURES IN A DIGITAL WORLD

*Orin S. Kerr**

119 HARVARD LAW REVIEW
(forthcoming December 2005).

How does the Fourth Amendment apply to the search and seizure of computer data? The Fourth Amendment was created to regulate entering homes and seizing physical evidence, but its prohibition on unreasonable searches and seizures is now being called on to regulate a very different process: retrieval of digital evidence from electronic storage devices. While obvious analogies exist between searching computers and searching physical spaces, important differences between them will force courts to rethink the basic meaning of the Fourth Amendment's key concepts. What does it mean to "search" computer data? When is computer data "seized"? When is a computer search or seizure "reasonable"?

This article offers a normative framework for applying the Fourth Amendment to searches of computer hard drives and other storage devices. It begins by exploring the basic differences between physical searches of physical property and electronic searches of digital evidence. It then considers how the Fourth Amendment should apply when a government investigator retrieves evidence from a person's computer, and concludes that exposing data to an output device such as a monitor should be a Fourth Amendment "search" ordinarily requiring a warrant. While copying data should not be deemed a seizure of that data, imaging a computer should be regulated by the Fourth Amendment and searches of copies should be treated the same as searches of the original. In the final section, the article considers ways to limit the scope of computer searches. The plain view exception may need to be narrowed or even eliminated in digital evidence cases to ensure that digital warrants that are narrow in theory do not devolve into general warrants in practice. Tailoring the doctrine in light of the new realities of computer investigations will protect the function of existing Fourth Amendment rules in the new environment of digital evidence.

* Associate Professor, George Washington University Law School. This is a September 7, 2005 draft; please do not quote without prior permission. Thanks to Michael Abramowicz, Stephanos Bibas, Susan Brenner, T.S. Ellis III, Laura Heymann, Adam Kolber, Chip Lupu, Marc Miller, Erin Murphy, Richard Myers, Mark Pollitt, Marc Rogers, Fred Rowley, Daniel Solove, Peter Smith, Bill Stuntz, Eugene Volokh, and participants in the law school faculty workshops at Duke, Emory, the University of San Diego, and the University of Georgia for comments on a prior draft.

INTRODUCTION

In the last decade, personal computers have become an increasingly important source of evidence in criminal cases. Computers record and store a remarkable amount of information about what users write, see, hear, and do. In a growing number of cases, searching a suspect's personal computer is an essential step of the investigation. The thorny issue for the courts – and the fascinating issue for scholars – is how the Fourth Amendment should regulate the process. How does the Fourth Amendment govern the steps that an investigator takes when retrieving evidence from a personal computer? At present, the answer is surprisingly unclear.¹ Lower courts have just begun to grapple with the issues, resulting in a series of tentative and often contradictory opinions that leave many answers unresolved.²

The problem is difficult because important differences exist between the mechanisms of physical evidence collection and digital evidence collection. The Fourth Amendment was drafted to regulate searches of homes and physical property, and has developed clear rules to regulate the enter-and-retrieve mechanism of traditional physical searches.³ Computer searches offer a very different dynamic: electric heads pass over billions of magnetized spots on metal disks, transforming those spots into data that is processed and directed to users via monitors. How can the old rules fit the new facts? For example, what does it mean to “search” computer data?

¹ While a number of law review articles have addressed isolated questions relating to computers and the Fourth Amendment, none have offered a comprehensive look at the meaning of searches, seizures, and reasonability in the context of digital evidence. Articles on the Fourth Amendment and computers more generally include Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches And Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39 (2001-2002); Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002); and Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75 (1994). For an explanation of existing doctrine, see UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, CH 1 & 2 (2002).

² See, e.g., *United States v. Maali*, -- F.Supp.2d --, 2004 WL 2656865 (M.D. Fla. 2004) (scope of computer warrant search); *United States v. Hill*, 322 F. Supp.2d 1081 (C.D. Cal. 2004) (Kozinski, J., by designation) (same); *In re Search of 3817 W. West End, First Floor, Chicago, Illinois 60621*, 321 F.Supp.2d 953, 958 (N.D. Ill. 2004) (requirements of computer warrants). These three cases are discussed in Section III, *infra*.

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

When is computer data “seized”? When is a search or seizure of computer data “reasonable”? The questions are particularly challenging because computers challenge several of the basic assumptions underlying Fourth Amendment doctrine. Computers are like wallets in a physical sense, homes in a virtual sense, and vast warehouses in an informational sense. Which insights should govern?

This article develops a normative framework for applying the Fourth Amendment to searches of computer hard drives and other electronic storage devices.⁴ It explores the various ways that the Fourth Amendment could apply to the retrieval of evidence from computers, and charts out a recommended path. The conceptual goal is to rethink Fourth Amendment doctrine to preserve the function of existing law in light of the new facts. To that end, the article attempts a pragmatist refitting of existing rules to the new technological practices. My hope is that the argument will prove helpful at several levels. At a doctrinal level, it articulates rules that courts can use in an important new set of cases. At a functional level, it explores how legal rules can adapt to new factual environments. Finally, at a more conceptual level it invites an understanding of how existing Fourth Amendment law is contingent on the mechanisms of physical evidence collection, as well as how different rule structures can implement various Fourth Amendment commands. Asking old questions in a new context offers a fresh perspective on the nature of Fourth Amendment law.⁵

The article contains three sections. Section I explores the four basic differences between the dynamics of traditional home searches and the new computer searches that trigger a need to rethink how the Fourth Amendment applies. First, home searches occur via physical entry and

⁴ This article focuses on searches of computer storage devices owned or exclusively used by suspects and stored locally. It does not address the surprisingly difficult questions raised by the application of the Fourth Amendment to remotely stored data. I plan to address the question of how the Fourth Amendment might apply to access of remotely stored data in my next article.

⁵ Professor Lessig has argued that when applying the Fourth Amendment to new technologies, courts should “translate” the original rules into something new to restore the old purpose in light of technological change. *See generally* Lawrence Lessig, *Fidelity as Translation*, 71 TEX. L. REV. 1165 (1993); LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999). My approach differs from Lessig’s in two basic ways. First, Lessig’s translation theory operates at a significantly higher level of generality. Lessig views the Fourth Amendment as a general command to protect privacy, and suggests that judges should interpret the Fourth Amendment in new technologies so as to protect privacy. *See id.* at 118. My approach attempts to rethink existing rules at a more particular level. Second, Lessig’s concern is constitutional fidelity; he aims to maintain fidelity to a set of constitutional commitments as technology changes. My concerns are more pragmatic. My interest lies in rethinking rules to retain the function of preexisting law, rather than to remain true to a conceptually correct interpretation of constitutional commands.

visual observation, while computer searches occur via passing an electric current over rotating magnetic points, processing the data and then outputting it. Second, home searches occur at the target's residence, while computer searches typically occur offsite on a government computer that stores a copy of the target's hard drive. Third, homes usually store only so much property, whereas computers can store entire virtual worlds of information often unbeknownst to the user. Fourth, homes are searched at a physical level, while computers generally need to be searched at both a physical level and a virtual level using a range of special programs for retrieving evidence that are inexpensive and very efficient. Each of these differences raises the prospect that rules established for physical searches may no longer be appropriate for digital searches.

Section II explores how the Fourth Amendment applies to the data acquisition stage of computer searches. It first considers the rules that should regulate looking through computer files, and contends that a Fourth Amendment "search" occurs whenever that data is exposed to human observation such as through a computer monitor. Under this approach, retrieving evidence from a computer ordinarily requires a warrant or an exception to the warrant requirement. The discussion then turns to the process of creating a "bitstream copy" or "image" of computer storage devices, a necessary step in most computer searches.⁶ Under existing law, generating a bitstream copy may be neither a search nor a seizure. This section argues that courts should reject such an outcome, and should regulate imaging as a search or seizure based on its interference with the owner's property rights. In addition, the same rules that regulate searches of originals should also apply to searches of copies.

Section III considers how Fourth Amendment applies to the data reduction stage of computer searches. The key question is how to limit the invasiveness of computer searches to avoid the digital equivalent of general searches. There are two basic approaches: *ex ante* restrictions articulated in warrants themselves, and *ex post* standards applied during judicial review. This section argues that *ex ante* restrictions are inappropriate given the highly contingent and unpredictable nature of the forensics process. To limit and regulate computer searches, the admissibility of evidence discovered beyond the scope of a warrant should be governed by a restrictive prophylactic rule applied *ex post*. While it is too early to tell exactly what rule is best – forensic tools, practices, and computer technologies are still evolving rapidly – the arrow of technological change points in the direction of tightening or even eliminating the plain view exception.

⁶ See notes [] to [], *infra*, and accompanying text.

By rethinking Fourth Amendment rules in the context of digital evidence, the article also offers a deeper perspective on the Fourth Amendment as a whole. It reveals the Fourth Amendment as a mechanism for regulating the information flow between individuals and the state. Existing law performs that function by mapping the doctrinal structure of “searches” and “seizures” onto the characteristics of physical property. Those physical barriers often are missing in a digital environment, and the question becomes how to regulate access to information without them. Working through how the Fourth Amendment might apply to computer searches reveals existing rules as contingent on the assumptions of the physical world. The digital world of computer data offers a particularly pure platform for the Fourth Amendment to operate: it offers an environment of pure data, and invites a reconsideration of how the courts can regulate the information flow between individuals and the state in a new factual environment.

I. THE NEW FACTS OF COMPUTER SEARCHES AND SEIZURES

The Fourth Amendment was enacted in response to the English and colonial-era experience with general warrants and writs of assistance.⁷ General warrants permitted the King’s officials to enter private homes and conduct dragnet searches for evidence of any crime.⁸ The Framers of the Fourth Amendment wanted to make sure that the nascent federal government lacked that power. To that end, they prohibited general warrants: every search or seizure had to be reasonable, and a warrant could issue under the Fourth Amendment only if it particularly described the place to be searched and the person or thing to be seized.⁹ Inspired by this history, the modern Supreme Court has used the text of the Fourth Amendment to craft a comprehensive set of rules regulating law enforcement that tends to reflect widely shared notions of the proper role of law enforcement.¹⁰ The textual requirement that searches and seizures must above all else be “reasonable” has permitted the Supreme Court to

⁷ See, e.g., NELSON B. LASSON, *THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION* 13-78 (1937).

⁸ See *id.* at 29.

⁹ 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.”).

¹⁰ See William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 553 (1992) (noting that Fourth Amendment rules “seem designed to approximate a negligence standard—to ensure that the police behave reasonably”).

craft a set of rules that balance law enforcement needs with individual interests in the deterrence of abusive law enforcement practices.¹¹

Over two hundred years after the Fourth Amendment was enacted, the search of a home remains the canonical fact pattern of a Fourth Amendment search and seizure case.¹² The Fourth Amendment rules governing the search of a house are well-settled. The act of entering the home triggers a “search” that invades the reasonable expectation of privacy of whoever lives there; the government can only enter the home if investigators have a warrant or an exception to the warrant requirement applies.¹³ Once legitimately inside the home, the police are free to walk around open spaces inside without a new “search” occurring.¹⁴ Opening cabinets or moving items does constitute a search, however; like the entry into the home, that search must be allowed by the warrant or an exception.¹⁵ If the police have a warrant, the warrant allows them to take away any evidence named in the warrant. The taking away of physical property is a “seizure,” and is reasonable if the property is named in the warrant.¹⁶ The police can also take away other evidence that they come across in plain view so long as the incriminating nature of the other evidence is “immediately apparent.”¹⁷ Viewed collectively, the rules that govern house searches effectively regulate privacy in the home.

Enter computers, and the world of digital evidence. The rise of computers in recent years has triggered the arrival of a new type of search: searches of computer data stored on computer hard drives and other storage devices. As computers become more closely integrated into our day-to-day lives, the importance of computer searches will only increase. The question is, how does the Fourth Amendment apply to retrieval of data from computer storage devices? Computer searches place considerable pressure on existing Fourth Amendment doctrine. The dynamics of computer searches turn out to be substantially different from the dynamics of home searches. Computers replace the enter-and-take-away dynamic of home searches with something more like copy, scan, and copy. Of course,

¹¹ See *id.* at 562 (“Innocent suspects would presumably agree to be subject to some types of searches and seizures, because they have an interest in reducing the level of crime, and permitting searches facilitates that goal. But they presumably also value freedom from capricious police conduct, and so would insist on some level of cause to justify intrusive police actions, and might bar some types of police action altogether.”)

¹² See *United States v. United States District Court*, 407 U.S. 297, 313 (1972) (“[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.”).

¹³ *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001).

¹⁴ *Maryland v. Macon*, 472 U.S. 463, 469 (1985).

¹⁵ *Arizona v. Hicks*, 480 U.S. 321, 325 (1987).

¹⁶ *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

¹⁷ *Horton v. California*, 496 U.S. 128, 136 (1990).

criminal cases involving voluminous paper documents have presaged these new facts in some ways. But such cases have been rare, and their rarity has permitted courts to avoid creating new rules to handle them.¹⁸ Computer searches have made the new dynamics routine rather than exceptional.

The process of retrieving evidence from a computer is known as the computer forensics process.¹⁹ It is mostly experts' work: computer forensics analysis typically is performed pursuant to a search warrant by a trained analyst at a government forensics laboratory.²⁰ Weeks or months after the computer was seized from the target's home, an analyst will comb through the world of information inside the person's computer to try to find the evidence justifying the search. She will use a range of software programs to aid the search, and the search itself can take many days and even weeks. While the programs are still evolving and their features change every year, the tools help analysts sift through the mountain of data in a hard drive and locate specific types or pieces of data. Often the analysts will find a great deal of detailed evidence helping to prove the crime; in a few cases, the search will come up empty. In a number of cases, the search for one type of evidence will result in the analyst stumbling across unrelated evidence of a more serious crime, which then will lead to criminal charges for the more serious crime.²¹

Computer searches and home searches are similar in many ways. In both cases, the police attempt to find and retrieve useful information hidden inside a closed container. At the same time, it turns out that the shift from home searches to digital searches also involves several key differences with important implications for legal rules. While most judges and lawyers have a vague sense that investigators "look through" computers, the process of searching computers turns out to be considerably different from the process of searching physical spaces. Understanding

¹⁸ See Kerr, *supra* note [], at 303, 307.

¹⁹ See, e.g., BILL NELSON, ET. AL., GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS 2 (2004) ("Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases.").

²⁰ See UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS Ch. 2 (2002) (hereinafter, "DOJ Manual") ("In most cases, investigators will simply obtain a warrant to seize the computer, seize the hardware during the search, and then search through the defendant's computer for the contraband files back at the police station or computer forensics laboratory."). This is particularly true in the context of federal investigations; state investigations are more likely to occur at the police station. In civil cases, forensic analysis typically is performed by private companies hired by the litigants.

²¹ See, e.g., United States v. Gray, 78 F. Supp. 2d 524, 530-31 (E.D. Va. 1999) (execution of a warrant to search a computer for evidence of computer hacking leads to discovery of child pornography images).

how the Fourth Amendment should apply to computer searches requires appreciating those differences. This section explores the four basic factual differences between home searches and computer searches: the environment, the copying process, the storage mechanism, and the retrieval mechanism.

A. The Environment: Homes vs. Hard Drives

The traditional focal point of Fourth Amendment law is physical entry into a home.²² Homes offer predictable, specific, and discrete physical regions for physical searches. Police can enter through a door or window and can walk from room-to-room. Most houses and apartments will consist of anywhere from 2 to 10 rooms, and the police can search each room first by visually observing each room and then by opening drawers and cabinets and looking through them. The basic mechanism is walking in to physical space, observing, and moving physical items so as to expose additional property to visual observation. Enter, observe, and move.

Computer storage devices are very different. Computer storage devices come in many forms: hard drives, floppy disks, thumb drives, zip disks, and many others.²³ All of these devices perform the same basic function: they store zeros and ones that computers can convert into letters, numbers, and symbols. Every number, letter, or symbol is understood by the computer as a string of eight zeros and ones. For example, the letter “m” would be stored by a computer as 01001101, and the number “6” as 00110110.²⁴ A string of eight zeros and ones representing a single letter, number, or symbol is known as a “byte” of information. The total storage available on a particular storage device is represented by the number of bytes it can store. For example, a 40 gigabyte hard drive can store roughly 40 billion bytes,²⁵ in other words, the hard drive stores the equivalent of about 320 billion zeros and ones.

²² See *United States v. United States District Court*, 407 U.S. 297, 313 (1972) (“[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.”).

²³ See JIM KEOGH, *THE ESSENTIAL GUIDE TO COMPUTER HARDWARE* 140 (2002).

²⁴ This is the standard ASCII format. See Daniel Benoliel, Comment, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology*, 92 Cal. L. Rev. 1069, 1082 (2004).

²⁵ I say “roughly” because computers use binary numbers, not decimal numbers. A gigabyte actually refers to 2 to the 30th power bytes, which is about 1.073 billion bytes. See, e.g., E. GARRISON WALTERS, *THE ESSENTIAL GUIDE TO COMPUTING* 12-13 (2001); *MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY* 491 (10th ed. 2001) (defining “gigabyte” as “1,073,741,824 bytes”).

The drive itself consists of several magnetized metal platters, something like magnetized compact disks, that contain millions and even billions of tiny individual magnetized points placed in concentric circles like growth rings of a very old tree.²⁶ The magnetized points either can be left in a magnetized state, which represents 1, or a demagnetized state, which represents 0.²⁷ Whenever the user enters a command that requires the computer to access data stored on the hard drive or write data onto the hard drive, the disks spin and magnetic heads are directed over that portion of the hard drive where the particular information is stored. The magnetic heads pass over the magnetized points on the platters, generating an electrical current.²⁸ That current is the signal representing the zeros and ones that can be inputted into the computer processor or outputted from it.

While houses are divided into rooms, computers are more like virtual warehouses. When a user seeks a particular file, the operating system must be able to find the file and retrieve it quickly. To do this, operating systems divide all of the space on the hard drives into discrete sub-parts known as “clusters” or “allocation units.”²⁹ Different operating systems use clusters of different size; typical cluster sizes might be 4 kilobytes or 32 kilobytes.³⁰ You can think of a cluster as akin to a filing cabinet of a particular size placed in a storage warehouse. Just as a file cabinet is known to store particular items in a particular place in the warehouse, so the operating system might use a cluster to store a particular computer file in a particular place on the hard drive. Each operating system keeps a list of where the different files are located on the hard drive; this list is known (depending on the operating system) as the File Allocation Table or Master File Table.³¹ When a user tells his computer to access a particular file, the computer consults that master list and then sends the magnetic heads over to the physical location of the right cluster.³²

²⁶ See Keogh, *supra* note 25, at 144, 153; CRAIG BALL, COMPUTER FORENSICS FOR LAWYERS WHO CAN'T SET THE CLOCK ON THEIR VCR 9 (2004), available at www.craigball.com/cf_vcr.pdf (last visited January 12, 2005).

²⁷ See Keogh, *supra* note 25, at 141.

²⁸ See *id.* at 142, 152.

²⁹ PETER STEPHENSON, INVESTIGATING COMPUTER-RELATED CRIME 99-100 (2000).

³⁰ See Keogh, *supra* note 25, at 147-49.

³¹ See HANDBOOK OF COMPUTER CRIME INVESTIGATIONS 137 (Eoghan Casey ed., 2002).

³² If a file is larger than the cluster size used by that operating system, the operating system will assign multiple clusters to that file. The operating system's master list would keep the list of the different clusters where parts of that file are stored, and when the file is accessed the heads will be brought to the different clusters one after the other so the file can be gradually assembled and presented to the user. See Keogh, *supra* note 25, at 149.

The differences between homes and computers prompt an important question: what does it mean to “search” a computer storage device? In the physical world, entering a home constitutes a search.³³ Observing each room does not constitute a new search, but opening containers and cabinets to look inside does.³⁴ The dynamic is enter, observe, and move. A police officer does not physically enter a computer, however; he does not physically move anything inside it; and he does not visually observe the zeros and ones. Retrieving information from a computer means entering commands that copy data from the magnetic disks, process it, and send it to the user. When exactly does a “search” occur?

B. The Copying Process: Private Property vs. Bitstream Copies

A second difference between physical and home searches concerns ownership and control over the item searched. When a police officer searches a home, the home and the property he is searching typically belongs to the target of the investigation. Indeed, some sort of legitimate relationship between the property searched and the defendant is needed to generate Fourth Amendment rights.³⁵ Once again, computers are different. To ensure the evidentiary integrity of original evidence, the computer forensics process always begins with the creation of a perfect “bitstream” copy or “image” of the original storage device saved as a “read only” file.³⁶ All analysis of the computer is performed on the bitstream copy instead of the original.³⁷ The actual search occurs on the government’s computer, not the defendant’s.

A bitstream copy is different from the kind of copy users normally make when copying individual files from one computer to another. A normal copy duplicates only the identified file, but the bitstream image copies every bit and byte on the target drive in exactly the order it appears on the original – including all files, the slack space, MFT, metadata, and the like.³⁸ Whereas casual users make copies of files when their machines are running, bitstream copies generally are created using special software after the computer has been powered down.³⁹ The bitstream copy then can

³³ See *Soldal v. Cook County*, 506 U.S. 56, 69 (1992) (“[T]he reason why an officer might enter a house . . . is wholly irrelevant to the threshold question whether the Amendment applies. What matters is the intrusion on the people’s security from governmental interference.”)

³⁴ See *United States v. Ross*, 456 U.S. 798 (1982).

³⁵ *Minnesota v. Carter*, 525 U.S. 83, 85 (1998) (requiring a substantial connection with a resident to grant a visitor to a home standing to challenge a search of the home).

³⁶ See *Nelson supra* note 21, at 50-51.

³⁷ See *id.*

³⁸ See *id.*

³⁹ Interview with Mark Pollitt, August 1, 2005.

be saved as a “read only” file, meaning that analysis of the imaged drive cannot alter it.

Once generated, the accuracy of the bitstream copy generally will be confirmed using something computer scientists call a “one way hash function,” or more simply, a “hash.”⁴⁰ A hash is a complicated mathematical operation performed by a computer on a string of data that can be used to compare two files to determine if they are identical.⁴¹ If two non-identical computer files are each inputted into the hash program, the computer will output wildly different results.⁴² If the two files are exactly identical, however, the hash function will generate exactly identical output. Matching output from the hash proves that all of zeros and ones of the two inputted files are exactly the same.⁴³ Forensics analysts can use these principles to confirm that the original hard drive and bitstream copies are identical. An analyst will enter data from the original and then data from the bitstream image into the hash function. Matching outputs from the hash function will confirm that the bitstream copy is an exact duplicate of the original drive.

The fact that computer searches generally occur on government property rather than the suspect’s raises important legal questions. First, what is the legal significance of generating the bitstream copy? Does that “seize” the original data, and if so, is the seizure reasonable? Relatedly, how does the Fourth Amendment apply to analysis of the copied data stored on the government’s computer? Does the retrieval of evidence from the government’s computer constitute a search? Or can the government search its own copy of data without legal restriction?

C. The Storage Mechanism: Home vs. Computer Storage

A third important difference between computers and homes concerns how much they can store and how much control people have over what they contain. Homes can store anything – including computers, of course – but as a general rule their physical size tends to limit the amount of evidence they can contain. A room can only store so many packages, and a home can only contain so many rooms. Further, individuals tend to have considerable control over what is inside their homes. Physical evidence can be destroyed, and a person usually knows when it is destroyed. Generalities are difficult, but in most cases these realities tend to limit the

⁴⁰ See Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1233-34 (2004).

⁴¹ See *id.*

⁴² *Id.*

⁴³ See *Peninsula Counseling Center v. Rahm*, 719 P.2d 926, 947-98 (Wash. 1986) (en banc) (Dolliver, C.J., dissenting) (discussing encryption and hash functions).

amount of evidence when the police wish to search a home. The home can only store items that fit in the home, and it can only store so many things; if a target suspects that the police are investigating him, he often can destroy at least some of the evidence before the police arrive.

Computers present a different picture. The types of evidence they can store are much narrower, of course. Computers can only store data. At the same time, the amount of data is staggering. Computer hard drives sold in 2005 generally have about 80 gigabyte storage capacities, roughly equivalent to 40 million pages of text or about the amount of information stored in the books located on one floor of a typical academic library. By the time you are reading this, these figures likely will be outdated: storage capacities of new computers tend to double about every two years.⁴⁴ At this rate, a new computer purchased in ten years will store about twenty trillion zeros and ones.⁴⁵ While computers are compact at a physical level, every computer is akin to a vast warehouse of information.

Computers are also remarkable for storing a tremendous amount of information that most users do not know about and cannot control. For example, forensic analysts often can recover deleted files from a hard drive.⁴⁶ They can do that because marking a file as “deleted” normally does not actually delete the file; operating systems do not “zero out” the zeros and ones associated with that file when it is marked for deletion.⁴⁷ Rather, most operating systems merely go to the master list of which clusters contain what files and mark that particular cluster (or clusters) as available for future use by other files. If the operating system does not use that cluster again for another file by the time the computer is analyzed, the file that was marked for deletion will remain at that cluster undisturbed. These details mean that a tremendous amount of data often can be recovered from the computer hard drive’s “slack space,” space left temporarily unused within a cluster.⁴⁸ It can be accessed by an analyst just like any other file.⁴⁹

⁴⁴ See Kerr, *supra* note 7, at 302.

⁴⁵ I reached this estimate by multiplying 320 billion (the storage capacity of a 40 gigabyte hard drive) by 32, or 2 to the 5th power.

⁴⁶ See, e.g., *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

⁴⁷ See *id.*

⁴⁸ Keogh, *supra* note 25, at 147. Data can be hidden in slack space because files often are smaller than the clusters that contain them. When a file is smaller than a cluster, the cluster will contain unused space. Just like a filing cabinet reserved for a particular topic may be only partially filled, the cluster may be only partially occupied with its associated file. See Ball, *supra* note 28, at 23-25. Unlike a filing cabinet, however, empty space in a cluster isn’t really empty. Because deleting a file does not actually erase the file, but merely marks it as available for rewriting, the temporarily used space may still contain pieces of previously “deleted” files. Analysts can look

Computer operating systems and programs also generate and store a wealth of information relating to how the computer and its contents have been used. As a person uses more programs on his computer, that information becomes broader and more comprehensive. For example, the popular Windows operating system generates a great deal of important metadata about exactly how and when a computer has been used.⁵⁰ Common word processing programs like Wordperfect and Microsoft Word generate detailed information about how particular word processing documents were created, including temporary files that permit analysts to reconstruct the development of a file.⁵¹ Word processing documents can also store data about who created the file, as well as the history of the file.⁵² Browsers used to surf the World Wide Web can store a great deal of detailed information about the user's interests, habits, identity, and online whereabouts, often unbeknownst to the user. Browsers typically are programmed to automatically retain information about what websites the user has visited in recent weeks; users often use this history to trace their steps or revisit a page the user enjoyed. Some of these pages may contain very specific information; for example, the web page that reports on the fruits of an Internet search engine query generally will include the actual search terms the user entered.⁵³

The different storage practices of computers compared to homes prompt an important legal question: how can the Fourth Amendment's rules limit and regulate the scope of computer searches? The Fourth Amendment was created to abolish general warrants and require searches

through the slack space and often find important remnants of previously stored and incriminating files.

⁴⁹ Walters, *supra* note 27, at 57.

⁵⁰ See Keogh, *supra* note 25, at 151. For example, newer versions of Windows contain a New Technology File System (NTFS) log file that maintains a detailed log of system activity to allow the operating system to be reconfigured in the event of a crash. The NTFS includes the Master File Table, which keeps records of where files are located, who created them, and what users have access rights to them. Nelson, *supra* note 21, at 90-94. The MFT also stores the so-called "MAC times" associated with each file: when each file was Modified, Accessed, and Created. Casey, *supra* note 33, at 134-36. MAC times are often important to determine when a particular file was created, or to help establish that it was not (or was) tampered. See *id.* The Windows operating system may also save detailed snapshots of how a computer was used in its "swap files," also known as "page files." See Ball, *supra* note 28, at 29. Stephenson, *supra* note 31, at 101-02.

⁵¹ Ball, *supra* note 27, at 30-31.

⁵² See Dan Gookin, *Word for Dummies* Ch. 2 (2003).

⁵³ For example, if a user enters a search for "assassinate" & "how to dispose of the body" into the popular Google engine, the URL for Google's report will be: [http://www.google.com/search?hl=en&q=%22assassinate %22+%22 how+to+dispose +of+a+body%22&btnG=Google+Search](http://www.google.com/search?hl=en&q=%22assassinate%22+%22how+to+dispose+of+a+body%22&btnG=Google+Search)

to be narrow. Can the rules that limit physical searches also apply to computer searches, or are new rules needed?

D. The Retrieval Mechanism

The fourth and final difference between home searches and computer searches concerns the techniques for finding evidence and the environment in which the search occurs. Physical searches occur in a defined physical space. Searching the space generally requires assembling and training a search team that requires several people to act together. Securing the home and searching its contents in a comprehensive way usually requires a great deal of resources. Once the police have searched the space for the item sought, the search is done, and the police can leave. The police only look where the evidence might be found; if they are looking for a stolen car, for example, they won't look inside a suitcase to find it.⁵⁴

Computer searches are different. The search ordinarily is performed in the government's lab by a single analyst, who uses a wide variety of techniques and tools to identify the evidence sought from the mountain of data stored in the device. No one technique is perfect; each one has strengths and weaknesses.⁵⁵ Further, the realities of computer forensic analysis dictate that there is no set amount of time that it takes an analyst to analyze a computer for evidence. According to Mark Pollitt, former Director of the FBI's Regional Computer Forensic Laboratory Program, analysis takes as much time as the analyst has to give it.⁵⁶ If the case is unusually important or the nature of the evidence sought dictates that a great deal or a specific type of evidence is needed, the analyst may spend several weeks or even months analyzing a single hard drive. If the case is less important or the nature of the case permits the government to make its case more easily, the investigator may spend only a few hours.⁵⁷ For an analyst, determining which approach to take usually requires both consultation with the warrant and consultation with the case agent. The forensic analyst ordinarily needs to know what kinds of searches the warrant will permit as matter of law, but also what type and amount of evidence is needed as a practical matter to prove the government's case in court.⁵⁸

⁵⁴ See *United States v. Ross*, 56 U.S. 798, 824 (1982).

⁵⁵ Interview with Mark Pollitt, August 1, 2005.

⁵⁶ Interview with Mark Pollitt, August 1, 2005.

⁵⁷ *Id.*

⁵⁸ *Id.* For example, in a child pornography case, the analyst may only need only to find a certain number of images. While it would be possible to spend weeks finding every single recoverable image stored in the hard drive, it would not advance the readily proven case.

In contrast to physical searches, digital evidence searches generally occur both at a “logical” or “virtual” level and also at a more difficult “physical” level. In most cases, the process is considerably more labor intensive and thorough than equivalent physical searches of a home. Consider a search for a picture file believed to be evidence of crime. An examiner might begin the search by conducting a “logical search” through the hard drive for files with extensions known to be used for image files, such as “.jpg.”⁵⁹ A “logical search” refers to a search through the virtual file structure set up by the operating system; the search will look through the files that the Master File Table has designated as files accessible to users of the computer.⁶⁰ The forensic analyst could direct his software to consult the Master File Table for any files with the extension .jpg, and then either list these files or automatically present “thumbnail” images of those files for viewing. Forensic software will generally allow the latter to be done easily through a simple command. For example, the current version of the EnCase forensic software has a feature called “Gallery View.”⁶¹ If an analyst selects a hard drive or folder to be analyzed and then clicks the “Gallery” button, the software will look for all files ending with a picture file extension and will present a thumbnail of those files automatically to the user.⁶²

This sounds easy, but ordinarily will not suffice. It is easy to change the extension of a file. To hide a picture, a user might take a file saved with a “.jpg” extension and resave it as a file with an extension common to a different kind of file such as “.doc” or “.wpd.”⁶³ A search for picture files based on the logical file extensions will no longer locate the file. To find the picture file, the analyst will have to conduct a search at a physical level instead of a logical level. This means that the search technique must look at all of the information stored on the physical hard drive, not just the information registered by the operating system and included in its file structure.⁶⁴ The distinction between physical searches and logical searches is a fundamental one in computer forensics: while a logical search is based on the file systems present on the hard drive as presented by the operating system, a physical search identifies and recovers data across the entire physical drive without regard to the file system.⁶⁵

⁵⁹ “JPG” refers to “Joint Photographic Experts Group,” a common compression algorithm that allows computers to store pictures files in a relatively small amount of space.

⁶⁰ See Keogh, *supra* note 25, at 144-46.

⁶¹ See Guidance Software, En Case Manual v.4.20 at 23 (2004).

⁶² See *id.*

⁶³ Nelson, *supra* note 21, at 488-93.

⁶⁴ See *id.* at 493-95.

⁶⁵ See United States Department of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement 15-16 (2004).

Software can search for image files at a physical level by searching for file headers characteristic of known types of picture files. A file header is a segment of data that informs the operating system about the associated file; in the case of a picture file, the file header would contain data indicating that the file is a photograph of a particular type and dimension.⁶⁶ The file header remains unchanged regardless of the extension a user might place on the file, allowing a physical level search to uncover picture files that a logical level search would not locate. In addition, file header characteristics can be located in slack space or in partially deleted files; a skilled analyst can then attempt to reconstruct the file and recover the associated picture.⁶⁷ The process can be tremendously time-consuming, however. Searching an entire hard drive for elements of file headers can take weeks, and it is easy for an analyst to overlook elements.⁶⁸

Analysts can also search for specific picture files by using the one way hash function mentioned earlier. For example, the common hash values of many known illegal images of child pornography have been collected into a single database by the National Drug Intelligence Center.⁶⁹ In cases involving child pornography, for example, an investigator can run hashes of the individual files stored on the computer and see if any match the hashes of the known images of child pornography. If there is a match between the hash of a known file in the database and a file located in the computer, the analyst can be confident that he has identified a particular image without actually viewing it. Once a picture file has been located, the analyst can record information retained by the operating system about the file, such as the MAC times and the folder in which it was found.

A search for text files would occur in ways roughly similar to a search for image files. The basic idea is to use any known characteristics of the file to search for data on the hard drive that matches those characteristics, and to conduct the search both at the logical level and at the physical level.⁷⁰ Exact search protocols are difficult to settle *ex ante*; good forensic analysis is an art more than a science. If investigators are looking for a particular type of file believed to be stored in a particular location or generated by a particular program, the analyst might begin by looking first at that location or program. More broadly, the analyst might begin by running a search through known files for a particular word or phrase associated with the file or information sought. After conducting a logical search, the next step might be to try a physical search for that same string of text. The physical search would look not just in assigned files, but more

⁶⁶ Nelson, *supra* note 21, at 493.

⁶⁷ *See id.* at 493-517.

⁶⁸

⁶⁹ Nelson, *supra* note 21, at 237.

⁷⁰ Nelson, *supra* note 21, at 380-385.

broadly throughout the entire hard drive. Searches also can be run with a predetermined allowed error rate to account for misspellings and abbreviations. For example, if an analyst is looking for information on “bookmaking,” a search for that exact text would miss any appearance of “boookmaking” or “bkmaking.” If the error rate is set at 50%, however, the software will note any word that contains 5 or more of the 10 letters in “bookmaking.”⁷¹

Analysts can also locate specific known program applications and files by running hashes of files stored on the drive or in a region of the drive and comparing those hashes to hashes of known files. The National Drug Intelligence Center has calculated common hash values of nearly every known application and operating system file.⁷² All of those hash values have been collected into a database known as Hashkeeper,⁷³ and many forensic analysts will have collected their own databases of hashes known to be associated with specific types of files. In a computer hacking case, for example, an analyst might compare the hashes of the files found on the computer to the hashes of known hacker tools. A match would reveal the presence of the hacker tools on the suspect’s computer without requiring the analyst to look through files on the hard drive one by one. Once a particular text file has been located, the analyst can record information retained by the operating about the file, such as the MAC times and the folder in which it was found.

Once again, it is not always this easy. Files can be encrypted, scrambling them into ciphertext.⁷⁴ Encrypted files cannot be read at all; they will seem like mere gibberish to the forensics tools, and cannot provide evidence for law enforcement. To be useful to law enforcement, the forensic analyst must attempt to decrypt the encrypted files or part of the hard drive. This can be done in different ways, depending on how the files are encrypted. In general, however, the analyst must attempt to either locate or guess the encryption “key” (usually a long string of numbers) to decrypt the encrypted files, or else find the “passkey” (usually a password)

⁷¹ This example is taken from Nelson, *supra* note 21, at 384-85. Many computer forensics programs have special tools to simplify the search in specific contexts. For example, EnCase has a feature that tabulates the MAC times of all of the files on a hard drive (or folder) and presents them in a histogram format. This tool allows an analyst to focus on files that were created, modified, or accessed on a particular day or during a particular time period. Assuming that this data has not been manipulated, the feature also allows an analyst to see a snapshot of the time periods in which the computer was heavily used. The software arranges the files by date, greatly simplifying the work of the analyst.

⁷² Nelson, *supra* note 7, at 237.

⁷³ *See id.*

⁷⁴ *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 Mercer L. Rev. 507, 530 (2005).

that can first decrypt the key and then allow the files to be decrypted.⁷⁵ In some cases, the key or passkey may be located somewhere in the hard drive; the forensic analyst must go searching through the hard drive for it. In other cases, the analyst must try to guess the key using special software.⁷⁶ Sometimes this will work, allowing the files to be decrypted. In other cases the analyst will be unable to decrypt the encrypted files and no evidence will be obtained.⁷⁷ The process of attempting to find a key or guess the key can take weeks, and often is not successful.

The difference between computer searches and traditional physical searches raises difficult questions about the rules that should govern computer searches and seizures. Generally it is more difficult to plan a computer search *ex ante*; the search procedures are more contingent than procedures for physical searches, and are more of an art than a science. The process can require a very time-consuming and invasive search in every case, and the costs of a comprehensive search are substantially lower. The question is, should these dynamics impact the rules that courts use to review the scope of computer searches -- and if so, how?

II. THE FOURTH AMENDMENT AND DATA ACQUISITION

The computer forensics process can be broken down into two basic steps: the data acquisition phase and the data reduction phase. In the data acquisition phase, a government investigator obtains access to the computer and collects the information to be searched. For example, a police officer might see a defendant's computer, walk over to it, and look through a few files. He might then decide to turn off the computer and image the entire hard drive in preparation for a subsequent off-site search. In the data extraction stage, the investigator begins with an image of the hard drive and attempts to locate particular evidence it contains. To borrow a physical metaphor, data acquisition refers to collecting the hay, and data reduction refers to looking through the haystack for the needle.

This section considers how the Fourth Amendment applies to the data acquisition stage of the computer forensics process. It considers two questions: first, the basic rules that should govern looking through a computer, and second, the rules that should govern creating a bitstream copy of a storage device for a subsequent search. The legal framework depends on our answers to the threshold questions of Fourth Amendment law: whether or when a "search" or "seizure" has occurred. Searches and

⁷⁵ *See id.*

⁷⁶ *See, e.g.,* Elec. Frontier Found., *Cracking DES: Secrets of Encryption Research, Wiretap, Politics & Chip Design* (1998).

⁷⁷ *See, e.g., See United States v. Scarfo*, 180 F.Supp.2d 572 (D.N.J. 2001).

seizures are presumptively unreasonable (and therefore unconstitutional) unless a warrant has been obtained or the facts fit within a narrow exception to the warrant requirement. In contrast, conduct that does not constitute a search or seizure remains unregulated by the Fourth Amendment.

This section proposes that the rules that govern looking through a computer should be governed by the Fourth Amendment's prohibitions on searches, and specifically what I term an "exposure-based approach" to searches. Under this approach, a search of data stored on a hard drive occurs when that data, or information about that data, is exposed to human observation. Any retrieval of information stored on a computer hard drive, no matter how minor, should be considered a distinct Fourth Amendment search. This approach focuses judicial attention on justifying the retrieval of evidence from computer storage devices. The exposure-based approach deemphasizes the hard drive as physical property, and also deemphasizes many of the technical details of what computers do 'behind the scenes.' It treats hard drives as virtual warehouses of information, and keys the doctrine to justifying the retrieval of individual pieces of information from the warehouse to zones of human observation. As a practical matter, it means that agents are generally prohibited from retrieving evidence from it unless they have a warrant or an exception to the warrant requirement applies. Further, in the case of a private search, agents can only view the exact information viewed by the private actor unless they first obtain a warrant.

The discussion then turns to the rules that should govern creating a bitstream copy of a suspect's computer. The issue proves quite difficult because copying information is neither a search nor a seizure under existing law. The existing definition of seizure is linked to notions of physicality; because creating a copy does not take away the original, copying apparently does not seize anything. As a result, current Fourth Amendment rules may not regulate the imaging process at all. Courts should reject this approach on policy grounds, and instead use the Fourth Amendment to impose limitations on creating bitstream copies of computers. There are multiple ways of adjusting existing doctrine to achieve such a result, and the precise path may not matter a great deal. On balance, however, the better path is to retain the existing definition of seizures and regulate imaging based on how it interferes with the computer that is imaged. Finally, the same Fourth Amendment rules that apply to searching a suspect's computer should also apply to searching the government's bitstream copy. Taken together, this approach places Fourth Amendment limits both on the creation of a bitstream copy and any subsequent search of that copy.

A. *Basic Rules for Looking Through A Computer*

The first stage in many computer search cases involves a government investigator looking through a computer that is already up and running. Perhaps the investigator is searching a home and stumbles across a computer.⁷⁸ Or perhaps a private party has found evidence of crime on a computer and turns it over to the police for further investigation.⁷⁹ In both cases, the investigator may want to look through a few files on the computer to see what information it contains. This section considers the Fourth Amendment rules that should apply to regulate the process.

The Supreme Court has defined a Fourth Amendment “search” as government action that violates a suspect’s “reasonable” or “legitimate” expectation of privacy.⁸⁰ In the context of physical spaces, searches generally refer to intrusions into private spaces. A house is searched when a government agent enters it; a package is searched when a government agent opens it.⁸¹ The basic framework posits that people ordinarily have a reasonable expectation of privacy in their homes and packages, and the act of breaking the seal between public spaces and the private home or package triggers a search. In physical space, physical entry into the home is the most common (although not exclusive⁸²) means of breaking down the barrier between public and private. It exposes the inside of the home to observation that is impossible from outside.

This basic framework provides an obvious starting point for understanding how the Fourth Amendment should apply to looking through a computer. The first step should be to compare computers to homes and sealed containers. First, much like persons generally have a reasonable expectation of privacy in their home, they should have a reasonable expectation of privacy on the contents of his personal hard drive. A suspect’s hard drive is his private property, and a defendant should have a reasonable expectation of privacy in his hard drive just as well as any other property.⁸³ Unusual circumstances may lead to a different

⁷⁸ See, e.g., *United States v. Turner*, 169 F.3d 84, 86 (1st Cir. 1999).

⁷⁹ See, e.g., *United States v. Runyan*, 275 F.3d 449, 464-65 (5th Cir. 2001)

⁸⁰ *Smith v. Maryland*, 442 U.S. 735, 739 (1979) (citing *Katz v. United States*, 389 U.S. 347, 362 (1967) (Harlan, J., concurring)).

⁸¹ *Wilson v. Layne*, 526 U.S. 603, 610 (1999) (search of a home); *United States v. Ross*, 456 U.S. 798 (1982) (search of a package).

⁸² See, e.g., *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001) (holding that use of a thermal imaging device from outside the home constitutes a search of the home because it permits an observer to observe details about the inside the home previously unknowable without physical entry).

⁸³ *United States v. Blas*, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990) (“[A]n individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container.”).

result,⁸⁴ but the basic starting point for applying the Fourth Amendment to a computer hard drive is clear and generally uncontroversial: the Fourth Amendment applies to the contents of a computer hard drive just as it does to any other private property.⁸⁵

Cases applying the Fourth Amendment to containers also provide a natural starting point for identifying the basic contours of what it means to “search” a computer. “Containers” are a well-defined category within Fourth Amendment law: the Supreme Court has gone out of its way to develop a set of rules that apply equally to all containers, protecting “a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim” the same as “the sophisticated executive with the locked attaché case.”⁸⁶ The foundational premise of the container cases is that that opening up the container constitutes a search of its contents; if a person has a reasonable expectation of privacy in the contents of a container, opening the container and seeing the contents violates that reasonable expectation of privacy.⁸⁷

Applying this approach to computer storage devices leads to the conclusion, adopted by a number of courts, that accessing the contents of a computer or other electronic storage device “searches” the device.⁸⁸ This is a good start, and likely an uncontroversial one. Accessing information from a computer breaks down the seal between public and private much like entering a home or opening a package. For doctrinal purposes, this is a

⁸⁴ *United States v. Lyons*, 992 F.2d 1029, 1031-32 (10th Cir. 1993) (ruling that a defendant does not retain a reasonable expectation of privacy in the contents of stolen computers).

⁸⁵ In some cases, this position has been reached explicitly. *See, e.g.*, *United States v. Runyan*, 275 F.3d 449, 459 (5th Cir. 2001) (reasonable expectation of privacy in computer disks); *United States v. Reyes*, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a digital pager); *United States v. Lynch*, 908 F. Supp. 284, 287 (D.V.I. 1995) (same); *United States v. Chan*, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (same). In most circuits, however, this has been implicit in decisions that focused on other questions. *See, e.g.*, *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (plain view and warrant case); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (warrant case).

Special circumstances may present a different situation. For example, courts have held that a person does not retain a reasonable expectation of privacy in stolen computers, *see, e.g.*, *United States v. Wong*, 334 F.3d 831 (9th Cir.2003), and one court has held that a person does not retain a reasonable expectation of privacy in computers obtained by fraud, *see United States v. Caymen*, 404 F.3d 1196, 1200-01 (9th Cir. 2005). Plus, this discussion assumes that the computer is not connected to a network at the time of the search. The application of the Fourth Amendment to computer networks raises a host of difficulties that I plan to address in a future article.

⁸⁶ *United States v. Ross*, 456 U.S. 798 (1982).

⁸⁷ *Id.* at

⁸⁸ *See* sources in note 73, *supra*.

powerful insight. It means, among other things, that accessing information from a computer ordinarily should be a Fourth Amendment “search” that requires a warrant or an exception to the warrant requirement. In general, an investigator who sees a suspect’s computer and starts looking through files is conducting a Fourth Amendment search.

This insight answers a great deal, but leaves two important questions open. The first is a question that is important mostly for purposes of civil liability:⁸⁹ If the general process of accessing information on a computer can constitute a search, exactly what step does so? At what stage does the search occur: when the hard drive heads read the data from the drive, when the data is collected by the computer, when the analyst can see the data, or at some other point? The second question concerns the zone or scope of a search. When a user retrieves data from a hard drive, how much of the hard drive has now been searched? This is an essential question because if particular government action constitutes a search of a given zone, then it does not need any additional justification to examine and analyze anything within that zone. The zone defines how much a search of A allows a subsequent search of B. I will begin with the first question, and then turn to the second question.

1) At What Stage Does A “Search” Occur?

When an investigator retrieves information from a computer hard drive, a number of things happen inside the computer. A magnet passes over the section of the computer hard drive that contains the relevant data, inducing a current in a wire that carries the signal away.⁹⁰ This generates a copy of the data, and the computer sends the copy to the computer’s central processing unit.⁹¹ The copy may be stored in various types of memory temporarily, and may be copied to another storage device, and is ultimately processed by the software running on the computer. The output that a user sees is a packaged and heavily processed version presented to the user by the operating system. At which of these stages does a “search” occur? Does a search of data occur when a copy of the data is generated for the computer to use as input? When the computer processes the data? When the computer outputs the data to a monitor or printer? If a forensic analyst performs a series of operations on a hard drive; copying, collecting,

⁸⁹ This is important primarily for civil liability because the government must observe information to use it in a criminal case. If the government is attempting to introduce evidence in a criminal case, the entire sequence of events leading to the exposure of information must have occurred. Identifying the precise point a search occurred could be useful for purposes of applying the fruit of the poisonous tree doctrine, but likely would not be outcome-determinative in most cases.

⁹⁰ See notes [] to [], *supra*.

⁹¹ See notes [] to [], *supra*.

and processing that data, *but never actually seeing it*, has that data been “searched”?

The best answer is that a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when the data is copied by the hard drive or processed by the computer. I will label this the “exposure-based approach” to interpreting Fourth Amendment searches. A range of arguments support it. First, focusing on the exposure of data most accurately transfers our physical world notions of searching to the context of computers. Entering a house is a search in physical space because it exposes to human observation the otherwise-hidden inside of the house.⁹² In the computer context, there is no need to focus the “search” inquiry on physical action like entry; the law can look directly to the exposure. The approach focuses doctrinal attention on the key question from the perspective of individuals and the police alike – whether and when a person’s information will be kept private or exposed and shared with the police. A computer is akin to a virtual warehouse of private information, and the exposure-based approach allows the courts to monitor and require justification for each retrieval of information from the warehouse. It imposes the Fourth Amendment as a barrier to the retrieval of information from non-observable form to observable form.

The exposure approach also reinforces the traditional Fourth Amendment concern with the scope of searches.⁹³ Defining searches as data exposure provides a simple and intuitive yardstick for measuring the scope of a search. A broad search is one that exposes more information; a narrow search exposes less. Other approaches de-link the measured scope from the actual level of intrusiveness of the government conduct. For example, imagine a search occurred whenever information was copied from the hard drive, even if that data was never exposed to a user. Under this definition, a broad search could occur that exposed little information, and a narrow search could occur that proved quite invasive. For example, a text query that searches only for the word “naked5yroid” anywhere on a hard drive may be comprehensive at a physical level – the entire hard drive must be scanned – but its invasion of privacy is fairly small. In contrast, obtaining a copy of a target’s diary from a known position on the hard drive may be narrow at a physical level but amount to a tremendous invasion of privacy. Treating the former as troubling but the latter as trivial makes little sense. A definition of search that focuses on the exposure of information in human-observable form best tracks the traditional Fourth Amendment concerns with the scope of searches.

⁹² Cf. *Kyllo*, 533 U.S. at 38-39 (use of a thermal imaging device that reveals the equivalent of what one would observe inside a home constitutes a search).

⁹³ See notes [] to [], *infra*.

The exposure approach also proves much easier to administer than the alternatives. It is far easier to humans to control and understand exposure than the technical functioning of a computer. Machines can be programmed in different ways to perform different tasks behind the scenes. For the most part, users are blissfully unaware of these details. A rule hinging on them would be hard to apply *ex ante*, and also difficult to judge *ex post*. Analysts would need to be aware of exactly when a hard drive was reading from particular places on a hard drive, and judges would need to understand these highly technical and contingent details as well. Many cases could require the consultation of technical experts to try to reconstruct exactly what bits from the hard drive were copied, and which ones were processed, even if they were captures for only a nanosecond and no record of them has been retained. The common law principle of “*de minimis non curat lex*” – the law does not concern itself with trifles – seems an appropriate response to such an abstract claim.⁹⁴

Although the Supreme Court has touched on the issue only tangentially, existing precedents appear to support the basic contours of the exposure-based approach. The most important case is *United States v. Karo*.⁹⁵ The defendant in *Karo* received what he thought were cans of ether to extract cocaine as part of a narcotics conspiracy. Unbeknownst to Karo, the police were investigating him and had replaced the ether in one of the cans with a radio transmitter that emitted a signal allowing the police to track its location. The Court of Appeals had held that transferring the transmitter to Karo was a Fourth Amendment search because the transmitter had the potential to reveal invasive information. The Supreme Court disagreed, emphasizing that the key question was whether the use of the technology actually conveyed information to the police:

[w]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. A holding to that effect would mean that a policeman walking down the street carrying a parabolic microphone capable of picking up conversations in nearby homes would be engaging in a search even if the microphone were not turned on. It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence.⁹⁶

⁹⁴ Cf. *Bart v. Telford*, 677 F.2d 622, 625 (7th Cir.1982) (Posner, J.) (noting that *de minimis non curat lex* applies to constitutional torts).

⁹⁵ 468 U.S. 705 (1984).

⁹⁶ *Id.* at 712 (citations and internal quotations omitted)

This information-focused approach is echoed by *Kyllo v. United States*,⁹⁷ where a thermal imaging device was used to pick up infrared radiation emitted from the surface of a home. Because infrared radiation varies as a function of surface temperature, measuring it can be used to create a thermal image of the surface of a solid. The Court held that the “hi-tech measurement of emanations from a house” to determine the temperature of the wall was a search.⁹⁸ Notably, however, every object emits infrared radiation. The radiation is everywhere; it’s just that the wavelength of the radiation cannot be detected by human eyes and must be detected using a machine.⁹⁹ For *Kyllo* to make sense, it must be the transformation of the existing signal into a form that communicates information to a person that constitutes the search. What made the conduct a search in *Kyllo* was not the existence of the radiation signal in the air, but the output of the thermal image machine and what it exposed to human observation. Applying *Karo* and *Kyllo* to computers strongly suggests that a search occurs when digital information is exposed to human observation, not when it is copied from the hard drive.¹⁰⁰

2) *The Zone of a Computer Search: Physical Box, Virtual File, Or Exposed Data?*

Having identified the moment the search occurs, we can now consider how broadly the search extends. When particular data from a particular hard drive is accessed, exactly what has been searched? The zone of a search determines how broadly or how narrowly particular government action eliminates privacy protection elsewhere in a space. This inquiry is often overlooked in the case of physical searches, for two reasons. First, the zone of a physical search is intuitive; it correlates neatly with what is hidden and what is exposed. As we will see, however, intuitions obvious in the physical world can lose their clarity in the context of computers. Second, the precise zone of a search is critical only when the government’s authority to conduct a search extends to one zone but not others. If the government’s authority to search covers multiple spaces – such as the case of a search warrant, which ordinarily permits searching all of the zones in the place to be searched that can fit the evidence described in the warrant – the precise boundaries of the zone don’t matter. If the authority to search is zone-specific, however, the zone will define the permissible scope of the search.

⁹⁷ 533 U.S. 27 (2001).

⁹⁸ *Id.* at 33. n.4.

⁹⁹ See J. M. Lloyd, *Thermal Imaging Systems 2* (1997).

¹⁰⁰ See also *Brower v. County of Inyo*, 489 U.S. 593, 596 (1989) (“[T]he Fourth Amendment addresses misuse of power, not the accidental effects of otherwise lawful government conduct”).

An example involving a physical search helps explain the stakes. Imagine that the police enter a house to look for drugs. Inside the house, they wander around various rooms. In one room, they find a suitcase and rip it open, revealing drugs. It is clear that the entry of the house was a search; a defendant has a reasonable expectation of privacy in the home. But importantly, merely entering the home does not constitute a legal “search” of everything inside it. The zone of the search is limited. If the police had legal cause to enter the home, that cause would entitle the police to wander around and observe whatever in the house was in plain view.¹⁰¹ The zone of the search in the physical world would not entitle the police to open closed containers such as the suitcase, however. Under existing law, the opening of a closed container inside the house constitutes a separate search.¹⁰² The zone of the initial search includes open areas of the home, but does not extend to the observation of other property in the home not exposed to observation.

How do these principles apply to searches of computer data? Three basic options exist; the zone could be defined by the physical storage device, the contents of a virtual file, or the exposed data. If the zone is the physical storage device, looking at data on a hard drive renders the entire storage device searched. If the zone is a file, then that file is searched but the rest of the computer is unsearched. Finally, if the zone is data itself, then exposure of data leaves all unexposed information unsearched.

Existing case law reflects both virtual file and physical device approaches to resolving the zone of a computer search. A good example of a virtual file approach is the Tenth Circuit’s opinion in *United States v. Carey*.¹⁰³ In *Carey*, a forensic analyst was conducting a search through a computer hard drive for evidence of drug sales. When he discovered an image of child pornography, the investigator abandoned the original search and began looking for other images of child pornography.¹⁰⁴ He subsequently opened a string of additional files containing child pornography. The court held that the first discovered image was admissible, but the subsequent opened files were beyond the scope of the warrant. The search for child pornography was valid, but the additional opening of unrelated files on the computer were additional searches.¹⁰⁵ The clear import is that the relevant unit of search, at least in a case of digital images, is an individual file. If you analogize a computer hard drive to a suitcase, each file is like its own zippered pocket in the suitcase. In a

¹⁰¹ *Maryland v. Macon*, 472 U.S. 463 (1985).

¹⁰² *United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978) (search of a footlocker in a room).

¹⁰³ 172 F.3d 1268, 1273-75 (10th Cir. 1999).

¹⁰⁴ *See id.*

¹⁰⁵ *See id.* at 1274.

sense, a computer is a container that stores thousands of individual containers in the form of discrete files.¹⁰⁶

The Fifth Circuit's decision in *United States v. Runyan*¹⁰⁷ offers an example of the alternative physical device approach. The defendant in *Runyan* had separated from his wife, and in a search of his property she found images of child pornography stored on several ZIP disks and floppy diskettes.¹⁰⁸ She then turned over the disks to the police, and the police conducted comprehensive analyses of the disks without a warrant that yielded many more images of child pornography beyond what the wife had seen. There was no record of what particular files the wife had observed, but the Fifth Circuit concluded it did not matter: having legally accessed a few files under the private search doctrine, she had "searched" the disks.¹⁰⁹ The container was the physical hard drive, and a search of some files on the container left the container open to further inspection. According to the Fifth Circuit, any additional analysis of the disks merely "expanded" the prior search.¹¹⁰ The fact that the police had opened different files did not matter, as the zone of the search was defined by the physical hard drive.¹¹¹

Which is better: the virtual file approach of *Carey*, or the physical storage device approach of *Runyan*? In my view, the virtual file approach is clearly preferable. Computers are searched to collect information that they contain. When assessing how the Fourth Amendment applies to the collection of information, courts should focus on that information rather than the physical storage device that just happens to contain it. Using the physical box as the common denominator of a computer search would also

¹⁰⁶ For a similar approach, see *United States v. Barth*, 26 F.Supp2d. 929, 935 (W.D. Tex 1998).

¹⁰⁷ 275 F.3d 449 (5th Cir. 2001).

¹⁰⁸ *See id.* at 455

¹⁰⁹ *See id.* at

¹¹⁰ *Id.* at 464.

¹¹¹ For a similar example, see *United States v. Slalina*, 283 F.3d 670 (5th Cir. 2002). An analogous issue was addressed but not resolved by the Supreme Court in *Walters v. United States*, 447 U.S. 649 (1980). In *Walters*, boxes containing reels of obscene films were sent to the wrong address. The recipients at the wrong address opened the boxes, noted that the labels were pornographic, and attempted to view portions of the film by holding it up to the light. They then contacted the FBI, and the FBI viewed the entire films on a projector. The question before the Court was whether by viewing part of the film, the recipients had "searched" the entire film. No majority view emerged. Four Justices said yes, viewing the film as the physical box, *see id.* at [] (Blackmun .J., dissenting); two Justices said no, viewing the film as the information it contained, *see id.* at [] (opinion of Stevens, J.); and three Justices either did not resolve the case on that ground or did not explain their rationale, *see id.* at [] (opinion of White, J.), [] (opinion of Marshall, J.).

lead to unpredictable, unstable, and even disturbing results. The amount of storage that can fit in a single physical box is increasing exponentially over time. As computers contain more and more information, it will become increasingly awkward, if not bizarre, to say that a second search through the contents of the computer simply examine the contents of the physical box in a more comprehensive manner than before. A single physical storage device can store the private files of thousands of different users. It would be quite odd if looking at one file on a server meant that the entire server had been searched, and that the police could then analyze everything on the server, perhaps belonging to thousands of different people, without any restriction. This all the more true in a networked world. The rise of computer networks will make the physical box of computers matter less and less. A single box may contain the files of thousands of people; on the other hand, a single file may be stored on several networked physical boxes. Some computer storage devices may not be stored in any boxes at all. Over time, it should become increasingly clear that the Fourth Amendment should track the information, not the physical box.

Having rejected the physical box as the common denominator, the next question is a subtle one not directly implicated in existing cases: is the proper denominator the virtual file or the exposed data? Existing cases tend to ignore this question because the cases mostly involve possession of digital images of child pornography, where the contraband image is both the exposed data and the file contents. The distinction between files and data collapses in this context. In other cases, however, the distinction will prove tremendously important. Imagine that an officer is executing a search warrant and comes across a computer that is up and running with the first page of a 100-page document on the screen. The officer wants to view the other 99 pages of the document to see if it reveals evidence of criminal activity. Let's imagine, however, that for some reason the officer cannot justify a "search" of the computer. Can the officer take the mouse and scroll down to read the rest of the 100 page file without conducting a search, or does publishing the rest of the document on the screen search that information?

I think the better answer is to use the common denominator of the exposed information. The scope of a computer search should be whatever information appears on the output device, whether that output device is a screen, printer, or something else. Under this approach, scrolling down a word processing file to see parts of the file that were previously hidden is a distinct search of the rest of the file. This approach works best for several reasons. First, it fits nicely with the exposure theory of searches. Once again, what matters is exposure to human observation. Second, virtual files are not robust concepts. Files are contingent creations assembled by operating systems and software. Third, much information stored on a

computer does not appear in a file.¹¹² If the law is keyed to files, how can it apply to information not stored in a file? Fourth, an analyst who takes a mouse, clicks, and pulls down the file to see parts of the file not previously exposed has done nothing different than another analyst who double clicks on a second file to open it. In both cases, the analyst is exposing information not previously exposed. Both should be treated as searches.

Notably, in most cases an exposure standard would not block police officers from viewing the entirety of large computer files. As noted earlier, authority to search often includes the authority to search multiple zones. Officers searching a house pursuant to a warrant don't need to get a new warrant every time they open a new box or cabinet; opening the box or cabinet is a new search, but one justified by the warrant. Under the exposure standard, the same rule would apply to observing unexposed portions of large computer files. The exposure approach is critical only when the officer has legitimately viewed part of the file but has no authority to conduct a new search through the rest of it. It would ensure that viewing the remainder of the file is treated as a distinct search.

B) Generating a Bitstream Copy

In most computer search cases, government investigators create a bitstream copy of the storage device and then search the image rather than the original. Resolving how the Fourth Amendment should apply to the creation of a bitstream copy is surprisingly difficult. At first blush, it seems sensible to say that generating an image "seizes" the information.¹¹³ According to the Supreme Court, "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."¹¹⁴ If generating a bitstream copy of a hard drive or storage device "meaningfully interferes" with the owner's possessory interest, then creating the copy constitutes a seizure requiring a warrant or an exception to the warrant requirement.

The issue turns out to be substantially more complex than that. Existing doctrine has taken a different course; under *Arizona v. Hicks*,¹¹⁵ merely copying information does not seize anything. As a result, a choice exists between two basic approaches. Under the first approach, the creation of a copy is neither a search nor a seizure. Under the second option, some doctrinal hook is found to ensure that generating a bitstream copy does count as a search or seizure, either by rejecting *Hicks* for digital

¹¹² See Part I.

¹¹³ See, e.g., Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches And Seizures: Some Unresolved Issues*, 11. 8 Mich. Telecom. & Tech. L. Rev. 39, 111-12 (2001-2002).

¹¹⁴ *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

¹¹⁵ 480 U.S. 321 (1987).

evidence or through some other approach. On balance, I think the better approach is the second one, but that courts should reach this result while retaining *Hicks*. Generating a bitstream copy should require a warrant or an exception, but because of the way it manipulates the machine rather than because it generates a copy per se. Finally, the Fourth Amendment rules that apply to originals should also apply to bitstream copies.

1) *Hicks and Other Precedents on Seizing Information*

In *Arizona v. Hicks*,¹¹⁶ a police officer was searching an apartment under exigent circumstances when he came across an expensive stereo system. He suspected that the stereo system was stolen, and wrote down the serial numbers of some of the stereo components. A quick call to headquarters confirmed a match between the serial numbers of the components in the apartment and the serial numbers of stereo components stolen during an armed robbery. The Supreme Court agreed that copying the serial numbers did not “seize” them:

We agree that the mere recording of the serial numbers did not constitute a seizure. To be sure, that was the first step in a process by which respondent was eventually deprived of the stereo equipment. In and of itself, however, it did not “meaningfully interfere” with respondent’s possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure.¹¹⁷

Although reproducing the data generated a copy of it, generating a copy of the data did not seize anything.

Lower courts have agreed with this approach in cases involving photocopies and photographs. In *United States v. Thomas*,¹¹⁸ a package sent via UPS ripped open during sorting, and revealed obscene magazines inside it. UPS employees called the FBI, and an FBI agent made photocopies of the magazine pages before resealing the package. The package was then given back to UPS, although it was not delivered because apparently the address was improper. The FBI agents then requested a warrant to seize the package, and attached the photocopies of the magazine pages to the affidavit. Thomas challenged the FBI’s conduct, claiming that photocopying the magazines seized them. The Tenth Circuit disagreed: “The materials herein remained in UPS’s possession and their delivery was unaffected since they were undeliverable. The materials were

¹¹⁶ 480 U.S. 321 (1987).

¹¹⁷ *Id.* at 324. (citing *Maryland v. Macon*, 472 U.S. 463, 469 (1985)).

¹¹⁸ *United States v. Thomas*, 613 F.2d 787 (10th Cir. 1980).

searched but not seized.”¹¹⁹ Similarly, in *Bills v. Aseltine*,¹²⁰ an officer took 231 pictures of the home where a warrant was being executed. The homeowner sued the officers, alleging that taking the pictures had seized images of their home in a way not permitted by the warrant. The Sixth Circuit relied on *Arizona v. Hicks* and rejected the claim, concluding that “the recording of visual images of a scene by means of photography does not amount to a seizure because it does not ‘meaningfully interfere’ with any possessory interest.”¹²¹

One district court has applied this rationale to the copying of computer files, albeit as an alternative holding in an unpublished opinion. In *United States v. Gorshkov*,¹²² FBI agents accessed the Internet account of a suspect and downloaded his files without obtaining a warrant. Relying again on *Hicks*, the district court concluded that this was not a seizure “because it did not interfere with Defendant's or anyone else's possessory interest in the data. The data remained intact and unaltered. It remained accessible to Defendant and any co-conspirators or partners with whom he had shared access.”¹²³

Some authorities construing Rule 41 of the Federal Rules of Criminal Procedure point in the opposite direction of *Hicks* and its progeny. Rule 41 is the rule governing search warrants; it grants federal authorities the power to obtain a search warrant to “search for and seize” evidence.¹²⁴ In a series of cases in the 1970s and 1980s, courts considered whether Rule 41 authorizes search warrants to obtain information, specifically in the context of installing pen register devices and performing “sneak and peek” searches.¹²⁵ Courts construed the Rule 41 power broadly, rejecting claims that such surveillance was impermissible because it did not “seize” anything. In rejecting those claims, they implicitly (and sometimes explicitly) indicated that recording information “seized” it.¹²⁶

¹¹⁹ *Id.* at 789.

¹²⁰ 958 F.2d 697 (6th Cir. 1992)

¹²¹ *See id.* at 707. (citing *Hicks*, 480 U.S. at 324).

¹²² 2001 WL 1024026 at *12 (W.D. Wash. May 23, 2001).

¹²³ *Id.* Another district court rejected the idea that making a bitstream copy of target's hard drive was a seizure of the entire hard drive, although the opinion is too cryptic to make much of the court's conclusion. *See United States v. Triumph Capital Storage*, 211 F.R.D. 31 (D. Conn. 2002) (holding that generating a bitstream copy “does not mean that [the forensic analyst] seized the entire hard drive,” but not stating what it *does* mean).

¹²⁴ Fed. R. Crim. Pro. 41(a).

¹²⁵ *See, e.g., United States v. New York Telephone*, 434 U.S. 159 (1977) (pen register); *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986) (sneak and peek warrant)

¹²⁶ *See, e.g., New York Telephone*, 434 U.S. at 170 (holding that Rule 41 “is broad enough to encompass a ‘search’ designed to ascertain the use which is being

The tight relationship between the Fourth Amendment and Rule 41 suggests that these cases provide at least some authority for the view that copying computer files should be treated as a “seizure.” At the same time, the context of these cases weakens their value. The greater power to enter a private space and remove property suggests a lesser power to enter a private space and merely observe; it would be odd if the police could do the former but not the latter. Courts may have construed “seizure” broadly in the Rule 41 context to avoid this odd result. At least as a matter of precedent, *Hicks* and its progeny seem to outweigh the Rule 41 cases for interpreting seizures of information.

2) *Should Creating Bitstream Copies Be A Search or Seizure?*

If generating a copy of information does not “seize” anything, the shift from physical evidence to digital evidence may trigger a significant expansion of police powers. In a world of physical evidence, the police generally need to take evidence away to obtain it. The definition of seizure is tied to the taking. In contrast, computer data is nonrivalrous: investigators can get a perfect copy without depriving the owner of the original.¹²⁷ Further, generating a copy does not seem to be a search; data normally is not exposed when it is copied, but rather is transferred from one computer to another.¹²⁸ If generating a copy is neither a search or seizure, the police may be able to generate bitstream copies without limits imposed by the Fourth Amendment.

This is a troublesome result. Permitting the government to make and retain copies of our private files simply seems inconsistent with our traditions. The idea that the government could freely generate copies of our hard drives and retain them in government storage indefinitely seems too Orwellian -- and downright creepy -- to embrace it as a Fourth Amendment rule. Perhaps such a rule could be moderated by restrictions on searching copies. If the same rules apply to searching copies that apply to searching originals, the police would be able to image computers but not search the images without a warrant. The difficulty with this rule is that it may be difficult or impossible to know whether investigators are complying with them. Bitstream copies are stored by the government on

made of a telephone suspected of being employed as a means of facilitating a criminal venture and the ‘seizure’ of evidence which the ‘search’ of the telephone produces.”); *Freitas*, 800 F.2d at 1455 (holding that the purpose of a “sneak and peek” warrant “was ‘to seize’ intangible, not tangible, property. The intangible property to be ‘seized’ was information regarding the status” of the place to be searched.”)

¹²⁷ Cf. Mark A. Lemley, *Ex Ante Versus Ex Post Justifications for Intellectual Property*, 71 U. Chi. L. Rev. 129, 143 (2004).

¹²⁸ Some small amount of meta-data would be exposed in most cases, however, and that information would be considered the fruit of a “search.”

government machines; the suspect has no way of controlling access to or use of the copy.¹²⁹

Courts could take two alternative strategies to reject this approach and regulate the imaging process under the Fourth Amendment. First, courts could depart from *Hicks* in the context of digital evidence, and hold that generating a bitstream copy constitutes a seizure because a machine-generated copy is more complete and invasive than the copying of visible numbers on the outside of a turntable.¹³⁰ Alternatively, courts could regulate imaging by focusing on the interference and manipulation of the machine instead of the copying itself. Imaging generally requires commandeering the computer, disabling access to and use of the computer for a matter of hours.¹³¹ The computer ordinarily will be “seized” during this time.¹³² Even the act of connecting a cable to an input/output port may be a Fourth Amendment search or seizure. Although the analogy is not exact, some circuit courts have held that inserting a key into a lock without opening the door constitutes a search.¹³³ Other courts have disagreed,¹³⁴ but the uncertainty at least suggests room in existing doctrine for the view that connecting a cable needed to transmit the data to the government’s machine constitutes a search.

As a practical matter, it probably makes little difference which path is chosen.¹³⁵ Either one would require a valid warrant or an exception to that requirement before the government could image a person’s computer. On balance, however, I think the latter approach is preferable.

¹²⁹ Thanks to Eugene Volokh for this point.

¹³⁰ Susan W. Brenner & Barbara A. Fredericksen, *Computer Searches And Seizures: Some Unresolved Issues*, 11. 8 Mich. Telecomm. & Tech. L. Rev. 39, 111-12 (2001-2002).

¹³¹ Interview with Mark Pollitt, August 1, 2005.

¹³² See *Illinois v. McArthur*, 531 U.S. 326 (2001) (blocking defendant from entering his house while the police obtain a warrant to search it is a temporary seizure); see also Brenner & Fredericksen, *supra* note 132, at 113..

¹³³ See *United States v. Concepcion*, 942 F.2d 1170, 1772 (7th Cir. 1991) (Easterbrook, J.); *United States v. Portillo-Reyes*, 813 F.2d 1353 1358 n.5 (9th Cir. 1975). In these cases, the police have a key in their possession, and attempt to determine if the key is associated with a particular lock to determine ownership of the lock or key. The police insert the key in the lock and turn it just a bit to see if the key will open the lock, but do not open the lock itself.

¹³⁴ See *United States v. Lyons*, 898 F.2d 210, 213 (1st Cir. 1990) (“We conclude that this course of investigation did not constitute a search, or at least, not an unreasonable search protected by the Fourth Amendment.”); *United States v. DeBardeleben*, 740 F.2d 440, 443-45 (6th Cir.1984).

¹³⁵ One possible difference concerns whether the Fourth Amendment regulates creating a copy of the copy. If copying constitutes a seizure, then copying the copy would implicate the Fourth Amendment; if the key question is interference with the owner’s property, copying the copy likely would not implicate the Fourth Amendment.

Departing from *Hicks* may inadvertently create a series of other problems. First, the resulting rule may be overbroad. Every computer file is a copy; the act of accessing data from a hard drive necessarily generates a copy of that data, even if only for internal purposes. If copying computer data seizes it, then use of a computer would seem to require constant seizing. There may seem to be an intuitive difference between generating a copy of data incidentally as a byproduct of how computers work and generating a copy for the purpose of generating a bitstream image, but it is difficult to turn that intuition into a legal rule.¹³⁶ As a result, a broad definition of seizure would encompass not only making a copy for government use, but also simply using the computer at any time.

A broad definition of seizure in the context of digital evidence also creates difficult questions concerning the permissible duration of the seizure. Existing Fourth Amendment doctrines often factor in the duration of a seizure when determining whether that seizure was constitutionally reasonable.¹³⁷ This makes sense for physical property: the time period of the seizure reflects how long the owner has been deprived of his property. But if generating a copy constitutes a seizure, what is the time period during which the data is seized? Until the data is erased, perhaps? This would be a difficult rule: as explained earlier, deleting files normally does not mean they are actually destroyed.¹³⁸

3) *Copies Versus Originals*

The final question is how the Fourth Amendment should apply to the forensic analysis of government-generated copies. There are two obvious choices: courts can treat searches of copies just like searches of originals, or else treat copies merely as data stored on government-owned

¹³⁶ One approach might make the mens rea the key question. Perhaps the intentional creation of a copy is different from the incidental creation of a copy. *Cf. Brover v. County of Inyo*, 489 U.S. 593, 596 (1989) (“[T]he Fourth Amendment addresses misuse of power, not the accidental effects of otherwise lawful government conduct”). At the same time, this seems to rub up against the general aversion to motive-based standards in Fourth Amendment law. *See Whren v. United States*, 517 U.S. 806, 812 (1996) (“Not only have we never held . . . that an officer’s motive invalidates objectively justifiable behavior under the Fourth Amendment; but we have repeatedly held and asserted the contrary.”) (citing cases).

¹³⁷ *See United States v. Place*, 462 U.S. 596, 709 (1983) (“Although we have recognized the reasonableness of seizures longer than . . . momentary ones . . . the brevity of the invasion of the individual’s Fourth Amendment interests is an important factor in determining whether the seizure is so minimally intrusive as to be justifiable on reasonable suspicion” and therefore constitutionally reasonable).

¹³⁸ *See* notes [] to [], *infra*. Finally, departing from *Hicks* requires defining the precise line where *Hicks* ends and the new rule begins. If copying a computer file constitutes a seizure, what about photocopying, or writing down information on paper?

property. Under the former approach, the restrictions on searching original carry over to searching the copy; under the latter, the government can search the copy without restriction. I contend that the best choice is to treat copies as originals. Courts should apply identical rules regardless of whether the data analyzed is the original version seized or a government-generated copy. This is an important point given that forensics analysts generally make a bitstream copy of files and analyze the copy instead of the original.¹³⁹ Under my approach, courts should find that the making of a bitstream copy is not an independent “seizure,” but that the rules for analyzing the copy on the government’s physical hard drive are no different from the rules for analyzing the original.

Existing precedents touching on this question are surprisingly difficult to find. A few cases have applied the Fourth Amendment to handcopied and photocopied documents, but their relevance is uncertain. For example, early Fourth Amendment opinions by Justice Holmes¹⁴⁰ and Judge Learned Hand¹⁴¹ forbade government use of copied documents when the originals had been illegally seized. While these cases may be read as extending the same protections to copies as originals, it is probably fairer to view them as antecedents to the modern fruit of the poisonous tree doctrine.¹⁴² More recently, several federal appellate cases involve motions to return photocopies of seized documents brought under Rule 41 of the Federal Rules of Criminal Procedure. These cases mostly involve the exercise of equitable powers to return property, however, and not the Fourth Amendment.¹⁴³ A possible exception is *Vaughn v. Baldwin*,¹⁴⁴ in which the Sixth Circuit held that the Fourth Amendment did not permit the government to photocopy and retain seized documents after the owner of the documents withdrew his consent to having government agents seize and then search the originals. The reasoning of *Vaughn* is cursory and unclear, however, rendering it of little help.¹⁴⁵

¹³⁹ See notes [] to [], *infra*.

¹⁴⁰ See *Silverthorne Lumber v. United States*, 251 U.S. 385 (1920) (Holmes, J.).

¹⁴¹ See *United States v. Kraus*, 270 F. 578 (S.D.N.Y. 1921) (L. Hand, J.).

¹⁴² See *Wong Sun v. United States*, 371 US 471 (1963).

¹⁴³ See Fed. R. Crim. Pro. 41(g). For examples of such cases, see *Mason v. Pulliam*, 557 F.2d 426 (5th Cir. 1977); *Sovereign News Co. v. United States*, 690 F.2d 569 (6th Cir. 1982).

¹⁴⁴ 950 F.3d 331 (6th Cir. 1991).

¹⁴⁵ Judge Nelson’s opinion focused on the government’s decision to wait for months before copying the documents, and then its refusal to return the documents after consent was revoked. Judge Nelson found this conduct “unreasonable” and therefore unconstitutional. See *id.* at 333-24. This sheds little light on whether looking through the copies would be a search.

The Fourth Amendment rules governing searches of copies may be unclear because copying has long required human exposure and involvement. When copying entails human observation, it will usually be clear that examining copied information does not violate the Fourth Amendment. Recall *Arizona v. Hicks*, in which a police officer copied serial numbers from stolen audio equipment. Having just recorded the information himself by hand, it seems obvious that the officer can look again at the piece of paper without violating the Fourth Amendment.¹⁴⁶ Computer-to-computer copying is different. The data remains hidden; copies are generated without exposing the information to human observation. The question is, does this make a difference? Should we treat the software that generates the copy like a person who “sees” the original, eliminating Fourth Amendment protection? Or is the absence of human exposure a critical difference?

While existing law does not provide an answer, existing practice may do so. Generating and analyzing bitstream copies is a routine part of the forensics process, but no court has ever analyzed searches of copies as different from searches of seizures. In the handful of cases where the courts noted that the analysis of a computer hard drive was performed on a copy, courts analyzed the permissibility of the search of the copy without suggesting it made any difference.¹⁴⁷ From a practical perspective, this is the best approach. All data is a copy. Computer hard drives work by generating copies; accessing a file on a hard drive actually generates a copy of the file to be sent to the computer’s brain for processing. More broadly, computers work by copying and recopying information from one place to another. From a technical perspective, it usually makes no sense to speak of having an “original” set of data. Given this, it would be troublesome and artificial to treat copies as different from originals.

Treating copies as originals also fits nicely with the exposure rule for searches and the *Hicks* rule for seizures. Once again, the key is access to data. It should not matter if data is copied, transferred, or otherwise manipulated. What matters is that a defendant had a reasonable expectation of privacy in data on his hard drive at one point, and that data was not abandoned or exposed to others. When a forensic analyst performs the necessary steps to evaluate a hard drive, the exposure of the information from the hard drive to an output device such as a monitor counts as a search regardless of whether the information was most recently stored as a copy or a more direct original.

¹⁴⁶ See notes [] to [], *infra*.

¹⁴⁷ See, e.g., *United States v. Triumph Capital Storage*, 211 F.R.D. 31 (D. Conn. 2002) (search of image); *United States v. Scott*, 83 F.Supp.2d 187 (D. Mass. 2000) (same); *Commonwealth v. Ellis*, 10 Mass.L.Rptr. 429 (1999) (same); *United States v. Gallo*, 55 M.J. 418 (C.A.A.F. 2001).

III. THE FOURTH AMENDMENT AND DATA REDUCTION

Having settled on the rules that govern the acquisition phase of the computer forensics process, we can now turn to the subsequent data reduction stage. At this phase, investigators search through an image of the defendant's computer for specific evidence related to a crime. In most of these cases, the police will have obtained a search warrant authorizing the search. The question is, what steps can the police take to find the evidence named in the warrant? What kind of search pursuant to a warrant is a "reasonable" search, and what kind of search is "unreasonable"? What rules should regulate *ex ante* what steps the police can take, and what rules should regulate *ex post* the admissibility of the files they discover?

The broad challenge is finding a way to regulate the invasiveness of computer warrant searches. The framers of the Fourth Amendment included a particularity requirement to disallow general searches; all warrants must describe *ex ante* the particular place to be searched and the particular person or things to be seized.¹⁴⁸ In the physical world, this requirement imposes a serious restriction on police conduct, as it regulates where in the physical world the police can go and what physical property they can seize. The police can only go a particular place, can only search for particular property, and can only look in spaces large enough that the property may be located in that space.¹⁴⁹

These rules offer less protection against invasive computer searches, however, and today's diminished protections are likely to shrink even more as technology advances. For a range of reasons, computer technologies may allow specific warrants in theory to become general warrants in practice. Computers tend to play an ever greater role in our lives as computer technologies advance, meaning that they are likely to record and store increasingly complete pictures of our daily experience. At the same time, the particularity requirement does less and less as the storage capacity of computer devices gets greater and greater.¹⁵⁰ Even if the property

¹⁴⁸ See U.S. Const. Amend. IV.

¹⁴⁹ *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("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 and the places in which there is probable cause to believe that it may be found.")

¹⁵⁰ See Kerr, *Digital Evidence*, supra note [], at 302-03 ("Given how much information can be stored in a small computer hard drive, the particularity requirement no longer serves the function in electronic evidence cases that it serves in physical evidence cases. Whatever remaining function it serves diminishes every year.").

described in the warrant is a very specific file or type of information, locating that information may require a broad search for technical reasons. These changes means that as time passes, rules created to prevent general searches for physical evidence may result in the equivalent of general searches for digital evidence. Probable cause to seize and search a computer will justify an extremely invasive search that uncovers a tremendous amount of information beyond the scope of the warrant.

There are two basic strategies for regulating and narrowing the invasiveness of computer searches to restore the function of preexisting rules for the new environment: *ex ante* restrictions and *ex post* restrictions. The *ex ante* strategy seeks to regulate computer searches by requiring warrants to articulate the precise steps that forensic analysts can take when they conduct the forensic process. According to this approach, computer warrants should state not just *where* the search will occur, and for *what*, but also *how* the search will occur. Requiring the warrant to articulate the approved search protocol can limit executive discretion and avoid general warrants. The *ex post* strategy relies instead on standards of review of the forensics process after evidence is found. Under this approach, the courts review the search process at the suppression stage after evidence has been found and the government seeks its introduction at trial.

This Section addresses both approaches. It begins by explaining why the environment of digital evidence raises special concerns that searches specific in theory will become general searches in practice. It then contends that *ex ante* restrictions are an inappropriate response to this problem given the highly contingent and unpredictable nature of the forensics process. The better approach is to reform rules regulating the admissibility of evidence *ex post*. Although uncertainty about the direction of technological change counsels caution, the best option ultimately may be to reconfigure the plain view doctrine for digital searches. Computer hard drives store a tremendous amount of private information that can be exposed in even a targeted search. If everything comes into plain view, the plain view exception threatens to swallow the rule. Narrowing or even eliminating the plain view exception may eventually be needed to ensure that warrants to search computers do not become the functional equivalent of general warrants.

A) Reasonableness and Physical Evidence Collection

Investigators looking for one type of evidence often come across something else incriminating. Perhaps an officer looking through a suspect's pocket for a driver's license instead finds drugs. Or perhaps an officer looking inside a car for drugs instead comes across a gun. In some cases, the discovery of the latter evidence is inadvertent. In others, the officer's conduct is a pretext search for the former designed to discover the

latter. Creating a legal rule to govern admissibility of the latter evidence is difficult because no clear line separates cases where use of the extra evidence simply helps the police fight crime from cases where use of the extra evidence encourages abusive law enforcement practices. On one hand, permitting the police to use the additional evidence can give the police a very valuable tool to gather evidence and fight crime. Allowing the police to use all the evidence they come across during a valid search gives them an extra mechanism to protect public safety, and with no added risk to privacy; after all, the police have already conducted the valid search.¹⁵¹ Denying the police the use of powerful evidence if they come across it legitimately during a search seems to punish the police for good police work and good fortune.¹⁵²

On the other hand, permitting the use of the additional evidence can encourage discriminatory and inefficient law enforcement practices. If the police know that they can use legal authority to search for *A* as a way of looking for *B*, they may embark on pretext searches and fishing expeditions.¹⁵³ When combined with the remarkable breadth of many low-level offenses,¹⁵⁴ the ability to engage in pretext searches may permit the police to target unpopular or politically powerless persons or groups for sustained scrutiny. Evidence that a particular person has committed a low level offense may be easy to obtain, giving the police tremendous power to execute invasive searches upon the target of their choosing. This discriminatory and inefficient practice was just the kind of misuse of government power the Fourth Amendment was created to stop. Indeed, while courts generally will not scrutinize subjective intent to assess the validity of Fourth Amendment searches and seizures,¹⁵⁵ the fear that legal rules may enable pretext or general searches still remains a key principle driving Fourth Amendment doctrine.¹⁵⁶

The “plain view” doctrine is the legal rule that balances these two competing concerns. In its current form, the plain view doctrine permits

¹⁵¹ See *Horton v. California*, 496 US 128 (1990).

¹⁵² See *Arizona v. Hicks*, 480 U.S. 321, 327 (1987) (noting “the desirability of sparing police, whose viewing of the object in the course of a lawful search is as legitimate as it would have been in a public place, the inconvenience and the risk--to themselves or to preservation of the evidence--of going to obtain a warrant” when evidence is discovered in plain view).

¹⁵³ See *Coolidge v. New Hampshire*, 403 U.S. 443, 460 (1971) (plurality opinion of Stewart J.).

¹⁵⁴ William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 Mich L. Rev. 505 (2001).

¹⁵⁵ See *Whren v. United States*, 517 U.S. 806 (1996).

¹⁵⁶ See *Horton v. California*, 496 U.S. 128 (1990) (rejecting subjective intent test for plain view but recognizing that the possibility of officers using plain view to execute pretext searches is a legitimate Fourth Amendment concern).

the police to seize evidence discovered during a valid search if the incriminating nature of the item to be seized, sufficient to create probable cause that the item constitutes evidence,¹⁵⁷ is immediately apparent.¹⁵⁸ The broad scope of the doctrine reflects a judgment call that the dynamics of physical evidence collection make the risk of pretext and dragnet searches relatively low. *Horton v. California*¹⁵⁹ provides a useful illustration. In *Horton*, the Supreme Court held that the plain view exception justifies a search even if the officer had a subjective intent to execute a pretextual search.¹⁶⁰ This rule was permissible because other aspects of physical evidence collection already served to thwart general searches. First, “[s]crupulous adherence” to the requirement that the police particularly describe the place to be searched and thing to be seized made it unlikely that police would use the plain view exception as a means to conduct general searches.¹⁶¹ Second, the scope of warrantless searches was limited by the fact that police could only look in places and containers large enough to contain the physical evidence sought.¹⁶² Both reasons were rooted in the dynamics of physical evidence collection.

2) Reasonableness and Digital Evidence Collection

The facts of the computer forensics process present a very different dynamic, with a significantly higher risk of general searches. This is true for several reasons. First, the virtual nature of digital evidence weakens or eliminates the two traditional limits on searches and seizures identified in *Horton*. In the case of searches with warrants, digital evidence diminishes the regulatory effect of the particularity requirement.¹⁶³ The particularity requirement reflects a physical concern: the thinking is that the law can limit searches by limiting where in the physical world the police search and

¹⁵⁷ See *id.* at

¹⁵⁸ See *id.* at

¹⁵⁹ 496 U.S. 128 (1990).

¹⁶⁰ *Id.* at 138-39.

¹⁶¹ *Horton*, 496 U.S. at 139-40 (arguing that the interest in “prevent[ing] the police from conducting general searches, or from converting specific warrants into general warrants, is not persuasive because that interest is already served by the requirements that no warrant issue unless it particularly describ[es] the place to be searched and the persons or things to be seized”, and that “[s]crupulous adherence to these requirements serves the interests in limiting the area and duration of the search that the inadvertence requirement inadequately protects.”) (internal quotations and citations omitted).

¹⁶² *Id.* at 140-41 (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)).

¹⁶³ See Kerr, *Digital Evidence*, *supra* note [], at 302-03 (“Given how much information can be stored in a small computer hard drive, the particularity requirement no longer serves the function in electronic evidence cases that it serves in physical evidence cases. Whatever remaining function it serves diminishes every year.”).

naming the object of the search. Search for data on a hard drive upsets these assumptions. A warrant to seize a computer hard drive is sufficiently particular under existing standards – the computer itself is small – but an entire virtual world of information may be stored inside it. And as time passes, this virtual world gets only larger; the storage capacity of new computer hard drives has tended to double every two years.¹⁶⁴ In the case of warrantless searches, digital evidence can be located anywhere. The police can no longer rule out particular places based on the physical dimensions of the evidence sought.

Second, computers appear to be playing an ever greater role in our lives, and recording a growing proportion of it. In the 1980s, computers were used primarily as glorified typewriters. Today they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and much more. As computers become involved in more aspects of our daily lives, they record more and more diverse information. Each new software application means a new aspect of our lives that our computers monitor and record. As Part I demonstrated, much of this goes on behind-the-scenes; users often do not realize how much information is being generated and saved. But all of the recorded information is available to the forensic analyst. As our computers do more and more, we may eventually approach a world in which most details of our lives are recorded and stored in perpetuity in our computers. Every minute and every keystroke may end up stored inside our machines in a way that can be reconstructed later by a forensic analyst with perfect accuracy.

Third, computer searches tend to be unusually invasive. A search for one type of digital evidence often reveals a tremendous amount of other evidence: a great deal comes into plain view. Of course, this can be true with many types of searches, including searches of homes. Few searches feature any type of surgical precision. At the same time, computers are somewhat different because invasive computer searches are much less expensive and less time-pressured than traditional physical searches. While comprehensive home searches are possible, their cost and inconvenience makes them the exception rather than the rule. A search team must be organized and trained; the location must be controlled during the execution of the search. In contrast, a single computer analyst can conduct a very invasive search through a computer at any time, without particular time pressure. The analyst can comb through the computer for months; the only limit is the time the analyst has to give the case. No search team is needed to take control of the search location and collect physical evidence room by room. Computer searches lower the cost and

¹⁶⁴ See Kerr, *Digital Evidence*, supra note [], at 302.

inconvenience of invasive searches, making such invasive searches the norm rather than the exception.

To some extent, the invasiveness of computer searches in the future will depend on the uncertain development of forensic technology. Computer forensics programs evolve every year, and their features change on a regular basis. Computer searches may be invasive today, but it's possible that they won't be in the future. We can imagine the possibility that someday a computer forensics tool will exist that efficiently searches a computer hard drive, returning only the evidence sought. This hypothetical "Perfect Tool" will magically locate evidence described in a warrant; the analyst will enter in the terms described in the warrant, and the tool will find just that evidence and nothing else. Alternatively, perhaps Perfect Tool will not exist in the future. Perhaps instead there will only be "General Tool," a program that always reveals everything incriminating stored inside a computer when any kind of search is conducted. It is too early to know for sure whether the future will bring Perfect Tool, General Tool, or some mix of the two – and yet our concerns about the risks of pretext and dragnet searches depend at least in part on which future unfolds.

Despite this uncertainty, it seems likely that computer searches will continue to be very invasive in the future. Perfect Tool sounds wonderful in theory, but is likely impossible in practice; new technologies always produce countertechnologies designed to thwart them. Police and sophisticated wrongdoers inevitably play a cat-and-mouse game between suspects trying to hide evidence and forensic analysts trying to find it. This dynamic makes unlikely that it will ever be possible to rule out a particular search completely. If Perfect Tool were invented, hackers would quickly devise a counterstrategy to disable it. The counterstrategy would impair Perfect Tool's ability to locate the evidence named in the warrant, requiring investigators to use something more like General Tool to locate it. Even a very rare use of such counterstrategies would trigger a legitimate law enforcement need for General Tool in many cases; investigators generally will not know *ex ante* whether the computer's owner took countermeasures to thwart government searches.¹⁶⁵ In this environment, Perfect Tool may not be possible. It therefore seems likely that tools closer to General Tool than Perfect Tool will be the norm in the future. While tools that offer the promise of Perfect Tool may be used, a need will always exist for something more like General Tool.

¹⁶⁵ Cf. *United States v. Gray*, 78 F. Supp. 2d 524, n.8 (E.D. Va. 1999) (noting that investigators cannot rely on file names to limit searches for computer files because they do not know if the computer owner attempted to hide his files by changing the file names.

For all of these reasons, the balance struck by existing law may need to be rethought in the future for the case of digital evidence. Many computers will contain a wealth of evidence of even low-level crimes, and probable cause to believe a person engaged in even just a minor offense may justify an exhaustive search of their hard drives that will expose many of their most secret doings to government observation. The existing plain view exception remains rooted in the contingent dynamics of physical evidence collection, indicating a need for rethinking the doctrine given the very different dynamics of digital evidence. The overall goal should remain the same: the law should attempt to balance the threat of general searches against the public benefit of recovering additional evidence. The question is, what rules can best serve that balance in the context of the computer forensics process?

B) Ex Ante Restrictions for Computer Warrants

One response to the new dynamics of the computer forensics process would be to require computer warrants to articulate *ex ante* the steps that the analyst must follow when searching the computer. The Supreme Court has rejected this approach for physical searches. While warrants must establish probable cause and particularly name the property to be seized and the place to be searched, the Supreme Court has rejected the position that they must include “a specification of the precise manner in which they are to be executed.”¹⁶⁶ “On the contrary,” the Supreme Court has stressed, “it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant” subject to *ex post* review for reasonableness.¹⁶⁷ Judicial review of searches pursuant to a warrant is imposed *ex post*, not *ex ante*.

In the last decade, however, a handful of courts and commentators have argued that computer warrants merit a “special approach”¹⁶⁸ that requires the government to articulate the search strategy that forensics specialists will follow during searches of computer hard drive.¹⁶⁹ The thinking behind these proposals is that requiring a judge to pre-approve the specific steps undertaken during the forensics process can limit its scope.¹⁷⁰

¹⁶⁶ *Dalia v. United States*, 441 U.S. 238, 256 (1979). In *Dalia*, the government obtained a warrant to conduct bugging surveillance, and the police executed the warrant by covertly entering the place to install the bug. In an opinion by Justice Powell, the Court rejected the idea that the warrant had to state *ex ante* that it permitted covert entry.

¹⁶⁷ *Id.*

¹⁶⁸ *United States v. Carey*, 172 F.3d 1268, 1275 n. 7 (10th Cir. 1999).

¹⁶⁹ See notes 131 to 142, *infra*.

¹⁷⁰ See notes 132 to 141, *infra*.

The initial allure is clear. If articulating a search protocol can limit the search that occurs, the resulting search is more likely to be narrow and particular. Unfortunately, however, it turns out that the *ex ante* strategy is deeply flawed. It wrongly assumes that prosecutors and magistrate judges have the knowledge needed to articulate search strategies before the search begins. The forensic process is too contingent and unpredictable to allow *ex ante* rules, however. Legal regulation of computer searches should be imposed *ex post*, not *ex ante*, just like regulation of physical searches.

1) *Computers and the “Special Approach”*

The idea of articulating a search strategy in a computer search warrant is sometimes said to derive from a Ninth Circuit Case from 1982, *United States v. Tamura*.¹⁷¹ In *Tamura*, the government seized boxes of documents and took them offsite for review. The documents contained some documents that were evidence of crime commingled with many innocuous documents, and the government seized all the documents because it would have been infeasible to search through all the boxes on the site. Judge Betty Fletcher’s opinion approved the seizure but offered a “suggest[ion]” for how the government could “generally avoid fourth amendment rights” in cases involving commingled documents: get prior permission to seize all of the documents and conduct an offsite search before actually doing so, so that “wholesale removal” is “monitored by the judgment of a neutral, detached magistrate.”¹⁷² In other words, judges should sign off on the wholesale seizure of documents so that overbroad seizures occur only if they are justified by practical concerns.¹⁷³

In an influential 1994 law review article, Raphael Winick took this idea and added an important twist.¹⁷⁴ Winick noted that computers used in criminal activity will contain a great deal of innocent material commingled with criminal evidence, and urged courts to apply “the *Tamura* rule” to computers.¹⁷⁵ So far, so good. The rub is that Winick’s vision of the *Tamura* rule was quite different than anything in *Tamura* itself. While *Tamura* merely required judicial approval of the wholesale seizure, Winick’s version of the *Tamura* rule required courts to articulate specific search protocols explaining exactly how the officers could search seized hard drives whenever tightly focused searches were not possible. Winick proposed the “basic principle . . . that before a wide-ranging exploratory search is conducted, the magistrate should require the investigators to

¹⁷¹ 694 F.2d 591 (9th Cir. 1982).

¹⁷² *Id.* at 596.

¹⁷³ *Id.*

¹⁷⁴ Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J. L. & Tech. 75 (1994).

¹⁷⁵ *See id.* at 106.

provide an outline of the methods that they will use to sort through the information.”¹⁷⁶ Although framed as merely an application of *Tamura*, Winick’s approach in fact urged a considerable shift in how courts regulate Fourth Amendment searches. The particularity requirement of the warrant clause requires the warrant to say *where* the search will occur, and for *what*, but has not been interpreted to require the warrant to specify *how* the search will be executed.¹⁷⁷

Despite the questionable provenance of the Winick approach, the Tenth Circuit relied on it in important dicta in *United States v. Carey*.¹⁷⁸ In *Carey*, an officer searching a computer pursuant to a warrant for evidence relating to narcotics came across images of child pornography. He abandoned the search for the evidence named in the warrant and began to search for additional images of child pornography. The *Carey* court concluded that the search for additional images was improper, and cited Winick and *Tamura* in support of a recommended “special approach”¹⁷⁹ to avoid discovering evidence outside the scope of the warrant in computer searches: “Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site,” the Court advised, “the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents.”¹⁸⁰ The Tenth Circuit reemphasized the point a year later in a similar case, *United States v. Campos*.¹⁸¹

Interest in including search protocols in warrants was heightened by the publication of the Justice Department’s 2001 manual, *Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigations*.¹⁸² The DOJ Manual suggested that it may be a “good

¹⁷⁶ See *id.* at 106-108.

¹⁷⁷ See *Dalia v. United States*, 441 U.S. 238, 256 (1979) (“[I]t is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant”). Nor does Winick’s approach involve the same set of Fourth Amendment concerns at issue in *Tamura*: while *Tamura* centered around the seizure of innocuous materials commingled with incriminating ones, Winick’s version is concerned with minimizing the amount of incriminating material outside the warrant that may be uncovered during a comprehensive search.

¹⁷⁸ 172 F.3d 1268 (10th Cir. 1999). See notes [] to [], *supra*.

¹⁷⁹ *Id.* at 1275 n.27.

¹⁸⁰ *Id.* at 1275. See also *United States v. Hunter*, 13 F.Supp.2d 574, 584 (D.Vt.1998) (“To withstand an overbreadth challenge, the search warrant itself, or materials incorporated by reference, must have specified the purpose for which the computers were seized and delineated the limits of their subsequent search.”)

¹⁸¹ 221 F.3d 1143, 1147 (10th Cir. 2000) (quoting *Carey*, 172 F.3d at 1275).

¹⁸² In the interests of full disclosure, I should acknowledge that I wrote this manual when I was a DOJ lawyer, under the direction of a number of other attorneys at the Justice Department.

practice” in some cases for affidavits to explain the search techniques used to search a computer pursuant to a warrant.¹⁸³ The DOJ Manual noted that “the Fourth Amendment does not generally require such an approach,”¹⁸⁴ but pointed to *Carey* and *Campos* as a sign that at least the Tenth Circuit preferred it. The combination of the DOJ Manual and *Carey* has led to a surge of recent litigation on the use of search protocols to cabin the scope of searches. In several cases, defendants have argued that the failure to articulate a search strategy renders the search warrant overbroad and therefore invalid.

These arguments have been met with mixed results, and outcomes appear to hinge in large part on the sense of individual judges as to how easy it is to search a computer hard drive for evidence. For example, in *United States v. Hill*,¹⁸⁵ the defendant in a child pornography case argued that the warrant’s failure to articulate a search strategy rendered the warrant invalid. Judge Kozinski, sitting by designation, rejected the argument on the ground that it was impossible to know *ex ante* where a file might be located or how it might be found.¹⁸⁶ Judges with greater confidence in their ability to recognize and require proper *ex ante* restrictions on computer forensic analysis have reached different results. In one recent case, a magistrate judge in Chicago simply refused to issue a warrant to search a computer for evidence of tax evasion without a search protocol.¹⁸⁷ Investigators had probable cause to believe that the defendant kept evidence of her tax evasion crimes on her computer stored in her apartment. The magistrate judge refused to issue a warrant without a search protocol settled beforehand, however.¹⁸⁸ The Court justified this on four grounds: first, that computer search and seizures start with seizures, then allow searches; second, computers generally have intermingled documents; third, computers can store a tremendous amount of information; and fourth, computer technology allow the government to conduct a highly targeted search if it chooses to do so.¹⁸⁹

¹⁸³ DOJ Manual, *supra* note 6, at Ch. 2, Part C, Subpart 3 (“When agents have a factual basis for believing that they can locate the evidence using a specific set of techniques, the affidavit should explain the techniques that the agents plan to use to distinguish incriminating documents from commingled documents.”).

¹⁸⁴ *Id.*

¹⁸⁵ 322 F. Supp.2d 1081 (C.D.Cal. 2004) (Kozinski, J.).

¹⁸⁶ *Id.* at 1090-91.

¹⁸⁷ *In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621*, 321 F.Supp.2d 953 (N.D.Ill. 2004.)

¹⁸⁸ *Id.* at 962-63.

¹⁸⁹ *See id.* at 959.

¹⁸⁹ *Id.* at 959-60. *See also* *United States v. Maali*, 346 F.Supp.2d 1226, 1265 (M.D. Fla. 2004) (upholding search despite lack of search protocols, on ground that “[w]hile it may be preferable and advisable to set forth a computer search strategy in a

2) *Rejecting Ex Ante Restrictions for Computer Warrants*

With this history and doctrine in mind, the normative question is ready to be answered: What should courts do with the search protocol requirement? The answer hinges on an important practical point: The computer forensics process is contingent, factbound, and quite unpredictable. Before an analyst starts analyzing a storage device, he normally will have little idea what operating system the computer is running; what software is on it; how that software was used; what else is on the hard drive; or whether the target took steps to hide, misname, or otherwise disguise files. Perhaps the defendant took no efforts to hide incriminating files; perhaps he changed file extensions, altered file headers, encrypted files, or took other steps to thwart the forensics process.

Nor will investigators necessarily know what forensic tool the particular analyst may choose to use when the analyst performs his search. Having all of this information is critical to knowing how the search can be executed in the most targeted way, however. Different forensic tools have different features, and different features mean that tasks that may be easy using one program may be hard using another. It is difficult to know what the particular search requires and what tools are the best to find the evidence without first taking a look at the files on the hard drive. In a sense, the forensics process is a bit like surgery: the doctor may not know how best to proceed until he opens up the patient and takes a look. The ability to target information described in a warrant is highly contingent on a number of factors that are difficult or even impossible to predict *ex ante*.¹⁹⁰

In light of these difficulties, judges approving warrants are poorly equipped to evaluate whether a particular search protocol is the best and most targeted way of locating evidence stored on a hard drive. Given the contingency of the process, even a skilled forensic expert cannot predict exactly what techniques are going to be necessary to find the information sought by the warrant. Most judges are not skilled computer forensic experts, of course. Like most lawyers, they tend to have only a vague sense of the technical details of how computers work. While Winick and the *Carey* court are right that many search techniques exist to target

warrant affidavit, failure to do so does not render computer search provisions unduly broad.”); *United States v. Barbuto*, 2001 WL 670930 (D.Utah April 12, 2001) (suppressing evidence sue to the absence of a search protocol).

¹⁹⁰ See *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (noting that agents executing a search for computer files cannot be “required to accept as accurate any file name or suffix and [to] limit [their] search accordingly” because criminals may “intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories”).

computer searches, they fail to realize that the details of what technique is the best to use in a specific case usually cannot be determined until the search occurs. Powerful search techniques exist, but whether they will work in a particular case depends on circumstances difficult to predict beforehand. Plus, warrant applications are *ex parte*; a judge must try to judge whether the search protocol is appropriate based only on the government's presentation of the empirical picture. It is generally impossible to know ahead of time what techniques are needed, and judges in *ex parte* proceedings are particularly unlikely to grasp the difficulties.

A requirement that courts approve search strategies *ex ante* therefore serves little purpose. The *Tamura* decision attempted to ensure that a judge approved overbroad seizures before or shortly after they occurred; the idea was that a judge could make the call as to whether an offsite search was required. That's a sensible rule: the Fourth Amendment prohibits unreasonable seizures, and seizing beyond the scope of probable cause may be reasonable if justified by practical concerns but not reasonable otherwise. Judges can review this step *ex ante* because it occurs only once, when the property is removed from the location of the search. Judges cannot exercise the same *ex ante* control over the forensics process, however. Analyzing a computer is a continuous process that can involve the performing of hundreds or even thousands of individual commands and steps. Judges cannot oversee them all. To perform that job competently, judges would need to stand alongside the forensics expert and approve each and every step as the situation evolved and the practical picture changed. The decision tree that an analyst might use to decide what steps to take is simply too long and complex for a judge to approve *ex ante*. To some extent, this is the rules versus standards debate: standards are judged *ex post* in a fact-specific way, while rules are applied *ex ante* with less fact-specificity.¹⁹¹ The computer forensics process calls for *ex post* standards, not *ex ante* rules.

Search protocols may be useful in specific circumstances. For example, searches of computers that may contain privileged documents present special concerns. Investigators may specify a search protocol to explain how the investigators will handle privileged documents.¹⁹² Similarly, searches of third party computers such as large computer servers

¹⁹¹ See generally Pierre J. Schlag, *Rules and Standards*, 33 UCLA L. Rev. 379 (1985); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 Duke L.J. 557 (1992); Cass R. Sunstein, *Problems with Rules*, 83 Cal. L. Rev. 953, 956-57 (1995).

¹⁹² See, e.g., *United States v. Neill*, 952 F. Supp. 834 (D.D.C. 1997) (search protocol for search to avoid privileged files); *United States v. Hunter*, 13 F. Supp. 2d 574 (D. Vt. 1998) (same).

raise unusual problems.¹⁹³ Such searches typically occur onsite, rather than offsite, and the search protocol attached to the warrant can explain to the server owner how the search will unfold.¹⁹⁴ The search protocol can be given to the server owner onsite to ensure him that the search will be narrow.¹⁹⁵ In general, however, review of search strategies should be performed *ex post*, not *ex ante*.

C) Rethinking the Plain View Doctrine

If *ex ante* search protocols cannot provide effective tools for neutralizing dragnet searches, what can? This section argues that the best way to neutralize dragnet searches is to rethink the plain view exception in the context of digital evidence. The dynamics of computer searches upset the basic assumptions underlying the plain view doctrine. More and more evidence comes into plain view, use of evidence beyond the warrant no longer requires a “seizure” of that evidence, and the particularity requirement no longer functions effectively as a check on dragnet searches. In this new factual environment, a tightening of the plain view doctrine may be needed to ensure that computer warrants that are narrow in theory do not become broad in practice.

This section discusses three possible ways of tightening the plain view doctrine for digital evidence searches. The first approach would narrow the plain view exception based on the circumstances of the search, such as the analyst’s subjective intent or the tool used. The second approach would narrow plain view based on the nature of the evidence discovered, permitting the use of some kinds of evidence and blocking other types. Both of these proposals seem promising at first, but prove quite difficult to apply in practice. The third proposal is more draconian: it would abolish the plain view exception entirely. The rule would allow forensic analysts to take necessary steps to locate evidence stored on a hard drive, but at the cost that evidence discovered beyond the warrant cannot be used against the defendant absent an application of the inevitable discovery doctrine. Ending plain view for digital searches is not an ideal solution, and may not be necessary today. But it may eventually prove to

¹⁹³ See, e.g., *Steve Jackson Games, Inc. v. United States Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993) (holding the Secret Service liable under the Electronic Communications Privacy Act and Privacy Protection Act for seizing computer servers and taking them offsite pursuant to a valid warrant).

¹⁹⁴ This practice is followed in light of *Steve Jackson Games, supra*.

¹⁹⁵ See *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (noting that a valid warrant “assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.”) (quoting *United States v. Chadwick*, 433 U.S. 1, 9 (1977)).

best the best way to restore the function of the Fourth Amendment in a world of digital evidence.¹⁹⁶

1) Approaches That Focus on the Circumstances of the Search

While there are many ways of narrowing the traditional plain view exception, one approach would be to factor in the circumstances of the search. For example, some might want to would overturn *Horton* and restore the inadvertence requirement, placing the emphasis on the analyst's subjective intent. Others might want to regulate the particular tools during the forensic search, such as by requiring the police to use particularly sophisticated or advanced forensic tools. Still others might want to permit plain view evidence when the specific forensic step that uncovered the evidence was "reasonable," but not if the step was unreasonable. All of these proposals have surface appeal, but on deeper reflection prove unpromising.

Two courts already have refashioned the plain view exception so that it focuses on the analyst's subjective intent in the context of computer searches. In *United States v. Carey*¹⁹⁷ and *United States v. Gray*,¹⁹⁸ forensic analysts looking for one kind of information came across digital images of child pornography. In *Carey*, the analyst stopped looking for drug evidence and began to look exclusively for child pornography;¹⁹⁹ in *Gray*, the analyst continued to look for evidence of computer hacking and just happened to come across more child pornography.²⁰⁰ In both cases, the courts followed the subjective intent of the officer to stay within or look beyond the scope of the warrant. Where the officer tried to look for

¹⁹⁶ For the purposes of this discussion, I assume that courts will take a somewhat holistic view of the role of plain view in the context of computer searches. Technically speaking, the plain view doctrine is a limitation on the government's right to seize evidence. It regulates seizures, not searches. See *Horton*, 496 U.S. at 134 ("If 'plain view' justifies an exception from an otherwise applicable warrant requirement, therefore, it must be an exception that is addressed to the concerns that are implicated by seizures rather than by searches."). Obtaining copies of computer files does not seize anything under *Hicks*, however. Because the police can obtain copies without seizing anything, it seems that the plain view doctrine technically does not regulate government use of discovered digital evidence. While this seems to true as a technical matter, it turns out that no court that has applied the plain view exception to digital evidence has recognized or even acknowledged it. For my purposes, I will assume this existing judicial practice continues. To the extent that courts do recognize this technical point, it seems to point only more strongly for doctrinal reform.

¹⁹⁷ 172 F.3d 1268 (10th Cir. 1999).

¹⁹⁸ 78 F. Supp. 2d 524 (E.D. Va. 1999).

¹⁹⁹ See *Carey*, 172 F.3d at 1275.

²⁰⁰ See *Gray*, 78 F.Supp.2d at 530-31.

evidence described by the warrant, the discovered images could be used;²⁰¹ where the officers ignore the warrant, the images were suppressed.²⁰²

The subjective approach followed by the *Carey* and *Gray* courts offers one significant advantage over the existing objective test: it turns the emphasis from a question judges are poorly equipped to answer (the reasonableness of a particular forensic step) to a question judges are better equipped to answer (witness credibility). Judges are familiar with physical world searches; they can understand how searches occur and what steps agents might take. Armed with this knowledge, judges can use objective tests to distinguish steps that are consistent with a search for evidence from steps that are characteristic of general searches. Judges have little sense of how to distinguish a reasonable forensics process from an unreasonable one, however. The technical details are too contingent and fluid. In this environment, a subjective test may serve as a second-best proxy for the objective test. While judges may be poorly equipped to assess whether in fact an analyst's steps are consistent with a targeted search, they will be better equipped to tell whether the analyst was at least *attempting* to conduct a good faith targeted search.

The subjective approach has a critical weakness, however. An officer's subjective intent may be difficult to know. Even if the officer testifies on the issue, it is difficult for a defense attorney to challenge such claims on cross-examination. This is particularly problematic in the computer context because government agencies can set policies that mandate very thorough forensic investigations. For example, the FBI has generally trained its forensic analysts to conduct highly comprehensive examinations; the default practice is to leave no digital stone unturned.²⁰³ This policy can create "General Tool" through practice instead of technology. When every step taken by an analyst is a question of routine policy, it becomes difficult to exclude evidence on the ground that the analyst was attempting to circumvent the warrant. This may have been the problem with *United States v. Gray*: in that case, the agent testified that he kept searching for evidence named in the warrant after repeatedly coming across other evidence because he was simply following FBI forensic policies.²⁰⁴ The existence of otherwise-laudable standardized practices makes the subjective intent approach much less helpful in practice than it first seems in theory.

²⁰¹ See *id.* (permitting use of files when the law enforcement agent "never abandoned his original search").

²⁰² See *Carey*, 172 F.3d at 1275.

²⁰³ Interview with Mark Pollitt, former Director of the FBI's Regional Computer Forensic Laboratory Program, August 1, 2005.

²⁰⁴ *Id.*

The next option is for the law to require the use of certain tools instead of others. If the police can conduct a search using either Perfect Tool or General Tool, for example, perhaps the law should require use of Perfect Tool. The problem with this approach is that it does not provide an obvious judicially manageable standard for the courts to apply. Dozens of different forensic programs exist, each with their own strength and weaknesses, and each with their different costs. The tools morph quickly over time, as do the latest techniques in hiding data, making *ex ante* guidance difficult to provide. Which tool would be the best in any situation depends on how the officer was trained, how the tool was used, what techniques might be used to try to thwart investigators, and what other tools were available at that particular time. Competing considerations such as cost and ease of use would also make it difficult for a court to impose the requirement that particular tools should be used at any particular time.²⁰⁵ Finally, it remains difficult to know for sure when a particular tool is needed. An investigator who uses Perfect Tool on a computer but comes up empty will never know whether General Tool might have uncovered something Perfect Tool did not. Given the many competing considerations and difficult choices among cost, ease of use, and effectiveness, direct regulation of the tools used in the forensics process presents an unmanageable challenge for courts.

Another possibility would hinge admissibility of plain view evidence on whether the particular forensic step that led to the evidence was reasonable or unreasonable given the government's needs, the privacy violation, and the relevant legal authority.²⁰⁶ If the government's search was reasonable, then the plain view evidence can be admitted; if it was not, it will be excluded. Such a case-by-case approach is an interesting option, but may be difficult for a court to apply. First, for reasons explored earlier, it may be difficult for courts to identify exactly when a particular step is reasonable or unreasonable.²⁰⁷ Second, this standard would require courts to apply the fruit of the poisonous tree doctrine in an unusual context in which the causal connection among steps is unclear.²⁰⁸ For example, imagine that an analyst performs an examination in 100 steps, and that step 100 produces evidence of an unrelated crime that is beyond the scope of the warrant. Assume that step 100 is constitutionally

²⁰⁵ *Cf. id.* at 529 n. 8 (“[A]s computer technology changes so rapidly, it would be unreasonable to require the FBI to know of, and use, only the most advanced computer searching techniques.”).

²⁰⁶ *Cf. Delaware v. Prouse*, 440 U. S. 648, 654 (1979) (noting that the reasonableness of a seizure depends on a balance of the invasiveness of the search with the government's legitimate needs).

²⁰⁷ See notes [] to [], *supra*.

²⁰⁸ See *Wong Sun v. United States*, 371 U.S. 471 (1962).

reasonable in isolation, but that steps 98, 95, 74, and 51 are not. To determine whether the evidence is admissible, the court would presumably need to find out the casual relationship between the earlier steps and step 100 to determine if the fruits of the latter are fruits of the poisonous tree. While such questions arise in the case of physical searches, judges understand the causal relationships of physical searches. The computer forensic process is much more of a complex technical art, and a contingent and highly fluid one at that. Applying the fruits doctrine may be much more complicated.

2) *Approaches that Focus on the Evidence Obtained*

Another approach that has considerable surface appeal would hinge admissibility of evidence on the type of evidence obtained and its usefulness in other prosecutions. Perhaps the plain view doctrine should permit the use of evidence for serious crimes, or only terrorist offenses, but not allow evidence to be used for low-level offenses. Professor Stuntz has made a suggestion along these lines in his recent essay.²⁰⁹ Stuntz suggests that one way to regulate secret surveillance practices such as delayed notice warrants and Internet searches would be to give the government the power to conduct the search, but then would “limit the range of crimes the government can prove by evidence discovered through that tactic.”²¹⁰ Applied to the computer forensics process, the rule might be that the government can use evidence discovered in plain view only in specific types of prosecutions. Perhaps they can be used only in terrorism cases, or perhaps only in terrorism cases, homicide cases, and child pornography cases. At its best, this approach would let the government use the evidence when the law enforcement need is a compelling one, and yet block government use for low level crimes when the government may be using the evidence merely to harass individuals.²¹¹

This is a possible approach, but also a problematic one. First, it is quite difficult to draw an *ex ante* line between compelling cases and low-level cases. We tend to know the difference when we see it, but it is surprisingly hard to draw the distinction using a legal rule. Say we are most worried about terrorism cases, and the rule is that the government can only use plain view evidence in terrorism cases. This prompts a difficult question: What is a “terrorism” case? There is no federal crime of “terrorism.” Instead, the U.S. code contains a number of criminal offenses that may be used in terrorism-related situations.²¹² Is any case that involves

²⁰⁹ William Stuntz, Essay, *Local Policing After the Terror*, 111 Yale L.J. 2137, 2185 (2002).

²¹⁰ *Id.* at 2184.

²¹¹ *See id.*

²¹²

any one of these crimes a terrorism case? Can any evidence offered to prove any of these crimes justify the introduction of plain view evidence, even if not particularly probative? Given that some of these statutes are worded quite broadly, does this mean that the government can use plain view evidence simply by raising one of the terrorism crimes as one of several charges in a multi-count indictment, even if the crime does not seem to be terrorism-related at an intuitive level?

Second, any rule that hinges governmental power on the type of offense creates a strong incentive for Congress to expand that category over time, watering down the protection. If plain view evidence is admissible only in terrorism cases, for example, Congress will have an incentive to broaden the category of terrorism crimes. This dynamic has occurred in the context of the Wiretap Act, which requires the government to prove that it is investigating one of a number of specific federal crimes before the FBI can wiretap a telephone.²¹³ The list began as a narrow list in 1968, when the Wiretap Act was passed. Over time it has expanded dramatically, and now includes essentially every federal felony offense that is prosecuted with any regularity.²¹⁴ Why? Because there are always going to be some instances involving any time of crime in which use of the evidence would be beneficial. All it takes is one compelling case involving a crime not on the list for Congress to expand the category to include all cases of the crime on the list.

Finally, settling on a list of specific types of crimes that qualify for admissible plain view evidence proves quite difficult. It is hard enough to come up with a single rule that best balances law enforcement concerns against fears of pretextual or abusive investigations for all crimes. Coming up with different rules for different sets of crimes is exponentially more complicated. Consider the case of child pornography offenses. On one hand, fears that possession of child pornography images is linked to actual child molestation might make child pornography crimes a prime candidate for the list of offenses that allow the introduction of plain view evidence. On the other hand, child pornography offenses are the most commonly prosecuted and most easily proved type of digital evidence crimes; given the current state of law and technology, concerns about pretext searches may be most justified in the case of a government agent obtaining a warrant for a low-level crime in an effort to see if he can find any child pornography on the suspect's computer.²¹⁵ The right balance to strike isn't clear; over time it may change; and there may be a different answer

²¹³ See 18 U.S.C. § 2516(1).

²¹⁴ See Jeffrey Rosen, *The Unwanted Gaze* [].

²¹⁵

for different types of child pornography offenses.²¹⁶ Courts seem poorly suited to draw such lines,²¹⁷ and legislative line-drawing seems destined to result in a broadening over time. While these objections do not rule out such a tailored approach, they provide reason to approach it with considerable caution.

3) *Abolishing the Plain View Exception?*

This brings us to the simplest but also most draconian approach: the plain view exception could be abolished for digital evidence searches. Courts could apply a very simple rule, suppressing all evidence beyond the scope of a warrant – or, in the case of warrantless searches, evidence unrelated to the justification for the search – unless the traditional independent source or inevitably discovery doctrine removes the taint.²¹⁸ This approach would permit forensic investigators to conduct whatever searches they deemed necessary, and to use General Tool or its equivalent

²¹⁶ In a thoughtful student note, David Ziff makes an argument that might impose such a rule without a need for legal reform. See David J.S. Ziff, Note, *Fourth Amendment Limitations on the Executions of Computer Searches Pursuant to a Warrant*, 105 Colum. L. Rev. 841 (2005). Ziff contends that the fact that the incriminating nature of discovered evidence must be “immediately apparent” to fall within the plain view exception limits the plain view doctrine in computer searches. See *id.* at 869. The incriminating nature of image files such as child pornography images is immediately apparent; the incriminating nature of text-based files such as a letter would be less immediately obvious. As a practical matter, this would end up permitting child pornography images to be used as plain view evidence in every case, but would make it less likely that other types of evidence would be so used.

One difficulty with Ziff’s argument is that computer searches generally occur off-site pursuant to repeated searches on the government’s imaged copy, rather than on-site in a single search. In the former environment, data may be viewed many times by several people over a long period of time. It is unclear whether the “immediately apparent” requirement would apply to the first discovery of the data, or also to subsequent discoveries. If the latter, the requirement may have less significance in the context of digital evidence. Second, a number of courts have construed the “immediately apparent” requirement less strictly than Ziff expects. These courts have admitted documentary evidence under the plain view exception even if the incriminating nature of the documents might require considerable analysis. See, e.g., *United States v. Khabeer*, 410 F.3d 477, 482 (8th Cir. 2005) (admitting receipts and identity documents beyond the scope of the warrant in a fraud case under the plain view exception); *United States v. Calle*, 1999 WL 313361 (9th Cir. 1999) (airline and bus tickets admissible under the plain view exception because officer could read the tickets and understand that the dates on them were inconsistent with defendant’s statements to officer); *United States v. Calloway*, 116 F.3d 1129, 11133 (6th Cir. 1997) (notes, bank receipts, and power of attorney admissible under plain view exception in search for evidence of aircraft piracy).

²¹⁷ See Kerr, *Constitutional Myths*, supra note [], at 857-87.

²¹⁸ See notes [] to [], *infra*.

however they liked, with the caveat that only evidence within the scope of the warrant normally could be used in court. Dragnet searches would be neutralized by ensuring that only evidence within the scope of proper authority could be used. Statutory privacy rules resembling the non-disclosure rule for grand jury testimony would presumably be needed to supplement this protection;²¹⁹ such rules could ensure that evidence beyond the scope of a warrant is not only never used in court, but also never disclosed.²²⁰

It is too early for courts or Congress to impose such a rule. Many of the characteristic dynamics of computer searches identified in this article are trends gradually becoming more significant with time. A decade ago, courts could simply and accurately analogize computers to other closed containers; today, the analogy seems a stretch; a decade from now, it will probably seem obviously flawed. Given the present state of technology, eliminating the plain view exception would be too severe. As time passes, however, I expect that to change. Decades from now, I predict, abolishing the plain view exception will become an increasingly sound doctrinal response to the new dynamics of digital evidence collection and retrieval.

In time, abolishing the plain view exception may best reflect the competing needs of privacy and law enforcement in light of the new reality of computers and the digital forensics process. Forensic analysis is an art, not a science; the process is contingent, technical, and difficult to reduce to rules. Abolishing the plain view exception would respect law enforcement interests by granting the police every power needed to identify and locate evidence within the scope of a warrant given the particular context-sensitive needs of the investigation. Forensics experts could take whatever steps they believe are necessary to recover the named evidence. At the same time, the approach protects privacy interests by barring the disclosure of any evidence beyond the scope of a valid warrant in most cases. It is an imperfect answer, to be sure, but may be the optimal rule. While forensic practices may be invasive by technological necessity, a total suppression rule for evidence beyond the scope of a warrant both removes any incentive for broad searches and neutralizes the effect of broad searches that occur. It regulates invasive practices by imposing use restrictions *ex post* rather than attempting to control searches *ex ante*,²²¹ offering a long-term second-best approach to regulating the computer forensics process. It

²¹⁹ Fed. R. Crim. Pro. 6(e).

²²⁰ Cf. Stuntz, *supra* note [], at 2184.

²²¹ Cf. Harold J. Krent, *Of Diaries And Data Banks: Use Restrictions Under The Fourth Amendment*, 74 Tex. L. Rev. 49, 75 (1995) ("Use restrictions accommodate the government's interest in obtaining information with individuals' interest in confining disclosure of private information as much as possible").

would allow the police to conduct whatever search they need to conduct (to ensure recovery) and then limit use (to deter abuses).

Notably, ending plain view would not mean that all evidence beyond the scope of warrant need be immune from use for all time. For one thing, the independent source and inevitable discovery rules would still apply to allow evidence to be used when the government could justify access to the evidence for independent reasons unrelated to the initial broad computer search.²²² Under these closely related doctrines, evidence can be used and even admitted in court when the government can show that it had some independent source for the same information or that it would have discovered the same evidence through other means.²²³ These doctrines would ensure that the police are not placed in a worse situation by finding evidence pursuant to a broad search, but that neither are they in a better position. For example, if the police searched a computer for tax fraud, and then came across child pornography, whether the police would be able to use the child pornography in a separate prosecution would hinge on whether they could show that they would have come across the evidence absent the unrelated investigation.

CONCLUSION

The new dynamics of computer search and seizure teach important lessons about the Fourth Amendment. For most of its first two centuries, the Fourth Amendment was used almost exclusively to regulate government searches of homes and packages. The mechanisms of home and container searches directed Fourth Amendment doctrine to focus primarily on the entrance to the space and containers. In a world of physical barriers, action that broke down those physical barriers became the focus of judicial attention. The world of digital search and seizure shows that these choices are contingent on the architecture of physical searches. As computer searches and seizure become more common in the future, we will begin to see 20th Century Fourth Amendment doctrine as a contingent set of rules that achieves the foundational goals of Fourth Amendment law given the dynamics of searching physical property. Those physical rules will be matched by a set of rules for digital searches and seizures that attempt to achieve the same purpose in a very different factual context.

Of course, this doesn't mean we should start from scratch. Many common principles will and should emerge. For example, the digital rules

²²² See *Murray v. United States*, 487 U.S. 533, 536-41 (1988) (explaining the independent source doctrine); *Nix v. Williams*, 467 U.S. 431 (1984) (discussing the inevitable discovery exception to the exclusionary rule).

²²³ See *Murray*, 487 U.S. at 536-41.

I recommend share a number of common themes with the physical rules: the exposure approach to searches offers a virtual version of the physical search approach. The two share a common definition of seizure, and both reject *ex ante* restrictions in warrants. At the same time, the shift to digital evidence should be accompanied by an openness to rethinking other doctrines and addressing new questions, such as the scope of computer searches, the rules for searching copies, and the plain view doctrine, so as to update existing rules to reflect the environment of digital evidence.

Katz v. United States famously attempted to bring Fourth Amendment law into the world of new technologies by introducing the “reasonable expectation of privacy” test. The new world of computer search and seizure sheds new light – and new skepticism – on *Katz*’s privacy-based focus. The concept of privacy doesn’t quite capture the purpose of Fourth Amendment rules, it suggests; privacy is best seen as an important byproduct of Fourth Amendment rules, not its goal. The perspective of computer search and seizure suggests that the deeper role of Fourth Amendment doctrine is regulating the information flow between individuals and the state. In a sense, the digital world of computer data is a particularly pure platform for the Fourth Amendment to operate: it offers an environment of pure data, and considers how the courts can limit and regulate law enforcement access to that data given the practical dynamics of how the data can be retrieved. Privacy results when the rules restrict access or use of that information, but the broader question is one of regulating government access to information. The dynamics of criminal investigations in physical space offer one set of answers to this question. The dynamics of investigations involving digital evidence offer another, however, and courts should be open to rethinking the physical rules for digital searches to achieve the broader purposes of the Fourth Amendment.