

SEARCHES AND SEIZURES IN A DIGITAL WORLD

Orin S. Kerr

TABLE OF CONTENTS

INTRODUCTION	532
I. THE NEW FACTS OF COMPUTER SEARCHES AND SEIZURES	536
A. <i>The Environment: Homes vs. Hard Drives</i>	538
B. <i>The Copying Process: Private Property vs. Bitstream Copies</i>	540
C. <i>The Storage Mechanism: Home vs. Computer Storage</i>	541
D. <i>The Retrieval Mechanism: Physical vs. Logical</i>	543
II. THE FOURTH AMENDMENT AND DATA ACQUISITION	547
A. <i>Basic Rules for Looking Through a Computer</i>	548
1. At What Stage Does a “Search” Occur?.....	551
2. The Zone of a Computer Search: Physical Box, Virtual File, or Exposed Data?	554
B. <i>Generating a Bitstream Copy</i>	557
1. <i>Hicks</i> and Other Precedents on Seizing Information	558
2. Bitstream Copies and the Fourth Amendment	560
3. Copies vs. Originals	562
III. THE FOURTH AMENDMENT AND DATA REDUCTION	565
A. <i>Reasonableness and Physical Evidence Collection</i>	566
B. <i>Reasonableness and Digital Evidence Collection</i>	568
C. <i>Ex Ante Restrictions for Computer Warrants</i>	571
1. Computers and the “Special Approach”.....	572
2. Rejecting Ex Ante Restrictions for Computer Warrants	575
D. <i>Rethinking the Plain View Doctrine</i>	576
1. Approaches That Focus on the Circumstances of the Search.....	577
2. Approaches That Focus on Future Uses of the Evidence Obtained.....	580
3. Abolishing the Plain View Exception?	582
CONCLUSION	584

SEARCHES AND SEIZURES IN A DIGITAL WORLD

Orin S. Kerr*

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 of unreasonable searches and seizures is now being called on to regulate a very different process: retrieval of digital evidence from electronic storage devices. Although obvious analogies exist between searching physical spaces and searching computers, important differences between them will force courts to rethink the key concepts of the Fourth Amendment. 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 tangible 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. Although 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 to the realities of computer investigations will protect the function of existing Fourth Amendment rules in the new environment of digital evidence.

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 the suspect's personal computer is an essential step in 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

* Associate Professor, George Washington University Law School. 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 Emory University, the University of San Diego, the University of Georgia, Duke University, and UCLA for comments on a prior draft.

retrieving evidence from a personal computer? At present, the answer is surprisingly unclear.¹ Lower courts have just begun to grapple with the question, resulting in a series of tentative and often contradictory opinions that leaves many answers unresolved.²

The problem is difficult because important differences exist between the mechanisms of physical and digital evidence collection. The Fourth Amendment was drafted to regulate searches of homes and physical property, and the courts have 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? When is computer data “seized”? When is a search or seizure of computer data “reasonable”? These questions are particularly difficult because computers challenge several of the basic assumptions underlying Fourth Amendment doctrine. Computers are like containers 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

¹ Although a number of law review articles have addressed isolated questions relating to computers and the Fourth Amendment, none has offered a comprehensive look at the meaning of searches, seizures, and reasonableness in the context of digital evidence. See, e.g., Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39 (2002); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75 (1994). For an explanation of existing doctrine, see COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, pts. 1–2 (2002) [hereinafter DOJ MANUAL], available at <http://www.cybercrime.gov/s&smanual2002.htm>.

² Compare *United States v. Maali*, 346 F. Supp. 2d 1226, 1246–47 (M.D. Fla. 2004) (holding that the absence of a detailed search strategy did not render a warrant insufficiently particular), and *United States v. Hill*, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (Kozinski, J., by designation) (declining to find a warrant overbroad because it did not include a search methodology), with *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 962–63 (N.D. Ill. 2004) (determining that a warrant to search a computer failed to meet the particularity requirement).

³ See Orin S. Kerr, Essay, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 290–92 (2005).

⁴ This Article focuses on searches of computer storage devices owned or used exclusively 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, which I plan to address in my next article.

rethink Fourth Amendment doctrine in order to preserve the function of existing law in light of new facts. To that end, this Article attempts a pragmatic refitting of existing rules to new technological practices. My hope is that the effort will prove helpful on several levels. At a doctrinal level, it articulates rules that courts can apply 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

This Article contains three parts. Part I explores 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 are conducted by physically entering and observing, while computer searches require passing an electric current over rotating magnetic points, processing the data, and then sending it to a monitor or other output device. Second, home searches occur at the suspect's residence, while computer searches typically occur offsite on a government computer that stores a copy of the suspect's hard drive. Third, home searches normally involve a limited amount of property, whereas computer searches involve entire virtual worlds of information. Fourth, unlike home searches, computer searches generally occur at both a physical and virtual level through the use of special programs designed to retrieve evidence. Each of these differences raises the prospect that rules established for physical searches may no longer be appropriate for digital searches.

Part II explores how the Fourth Amendment applies to the data acquisition stage of computer searches. It first considers the rules that

⁵ Professor Lawrence Lessig contends that courts should "translate" constitutional commands when applying the Constitution to new technologies, restoring their original purpose in light of technological change. See generally LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165 (1993). My approach differs from Professor Lessig's in two important ways. First, Professor Lessig's concern is constitutional fidelity, while my own is more pragmatic. My assumption is that existing Fourth Amendment doctrine reflects widely shared notions of the need for reasonable restrictions on police investigations, and that those notions exist regardless of whether investigations involve searching a home or searching a computer. As a result, my interest lies in finding sensible rules that reflect these widely shared beliefs given the new factual environment, rather than in remaining faithful to a conceptually correct interpretation of a constitutional command. The second significant difference between Professor Lessig's approach and my own is the level of generality. Professor Lessig views the Fourth Amendment as a general command to protect privacy and suggests that judges should interpret the Fourth Amendment with respect to new technologies so as to protect privacy. See LESSIG, *supra*, at 118. My approach attempts to rethink existing rules at a more particular level.

should regulate looking through computer files, and contends that a Fourth Amendment “search” occurs whenever data is exposed to human observation, such as through a computer monitor. Under this standard, retrieving evidence from a computer ordinarily should require a warrant or an applicable 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. Generating a bitstream copy may be neither a search nor a seizure under existing law; this Part argues that courts should reject this approach and should instead regulate imaging as a search or seizure based on its interference with the owner’s property rights. In addition, courts should apply the same rules that regulate searches of originals to searches of copies.

Part III considers how the 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 creating the digital equivalent of general searches. There are two basic approaches: *ex ante* restrictions articulated in warrants and *ex post* standards applied during judicial review. This Part argues that *ex ante* restrictions are inappropriate given the highly contingent and unpredictable nature of the forensics process. To limit and regulate computer searches, a restrictive rule applied *ex post* should govern the admissibility of evidence discovered beyond the scope of a warrant. Although it is too early to tell exactly which 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 for digital evidence.

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 the digital environment, so the question becomes how to regulate access to information in their absence. Studying how the Fourth Amendment might apply to computer searches reveals existing rules as contingent on the assumptions of the physical world. The context 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 the 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 experiences with general warrants and writs of assistance.⁶ General warrants permitted the King's officials to enter private homes and conduct dragnet searches for evidence of any crime.⁷ The Framers of the Fourth Amendment wanted to make sure that the nascent federal government lacked that power.⁸ 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.¹⁰ The textual requirement that searches and seizures must above all else be "reasonable" has permitted the Supreme Court to craft a set of rules that balances law enforcement needs with individual interests in the deterrence of abusive law enforcement practices.¹¹

Over two hundred years after the enactment of the Fourth Amendment, the search of a home remains the canonical fact pattern of a Fourth Amendment search and seizure case,¹² and the rules for such a search are well settled. The act of entering the home triggers a "search" that invades the reasonable expectation of privacy of whoever lives there;¹³ the government can only enter the home if investigators have a warrant or an exception to the warrant requirement applies. Once legitimately inside the home, the police are free to walk around

⁶ See NELSON B. LASSON, *THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION* 79-105 (1937).

⁷ See *id.* at 25-27.

⁸ See *id.* at 94-95.

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").

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

open spaces.¹⁴ Opening cabinets or moving items triggers a new search, however; like entry into the home, those actions must be justified by the warrant or an exception.¹⁵ If the police have a warrant, the warrant allows them to take away any evidence it describes. The taking away of physical property constitutes a “seizure,” and it 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 evidence is “immediately apparent.”¹⁷ Viewed collectively, the rules that govern home searches effectively regulate privacy in the home.

Enter computers and the world of digital evidence. The widespread use of computers in recent years has led to a new type of search: searches of 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 the 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, 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 computer forensics.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

¹⁴ Cf. *Maryland v. Macon*, 472 U.S. 463, 469 (1985) (stating that a police officer’s examination of wares that were “intentionally exposed to all who frequent the place of business” did not constitute a search).

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

¹⁶ *United States v. Jacobsen*, 466 U.S. 109, 113–14 (1984).

¹⁷ *Horton v. California*, 496 U.S. 128, 136 (1990) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 446 (1971)) (citing *Hicks*, 480 U.S. at 326–27).

¹⁸ See Kerr, *supra* note 3, 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 DOJ MANUAL, *supra* note 1, at 63 (“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

months after the computer has been seized from the target's home, an analyst will comb through the world of information inside the computer to try to find the evidence justifying the search. She will use a range of software programs to aid the search, which can take many days or even weeks to complete. These tools help analysts sift through the mountain of data in a hard drive and locate specific types or pieces of data. Often they will uncover 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 evidence of an unrelated 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, significant differences exist. 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 how the Fourth Amendment should apply to computer searches requires appreciating those differences. This Part explores 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. Investigators can enter through a door or window and can walk from room to room. They can search individual rooms by observing their contents, opening drawers and other containers, and looking through them. The basic mechanism is walking into a physical space, observing, and moving items to expose additional property to visual observation. Enter, observe, and move.

Computer storage devices are different. They come in many forms, including hard drives, floppy disks, thumb drives, and Zip disks.²³ All of these devices perform the same basic function: they store zeros and ones that a computer can convert into letters, numbers, and symbols. Every letter, number, or symbol is understood by the computer as a string of eight zeros and ones. For example, the upper-case letter "M"

more likely to occur at the police station. In civil cases, the litigants typically hire private companies to perform forensic analysis.

²¹ See, e.g., *United States v. Gray*, 78 F. Supp. 2d 524, 526–28 (E.D. Va. 1999) (execution of a warrant to search a computer for evidence of computer hacking led to discovery of child pornography).

²² See *United States v. U.S. Dist. Court*, 407 U.S. 297, 313 (1972).

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

is stored by a computer as “01001101,” and the number “6” as “00110110.”²⁴ Each string is known as a “byte” of information and the number of bytes represents the total storage available on a storage device. For example, a forty gigabyte hard drive can store roughly forty billion bytes, or about 320 billion zeros and ones.²⁵

The hard drive itself consists of several magnetized metal platters, something like magnetized compact discs, that contain millions or even billions of tiny magnetized points placed in concentric circles like the growth rings of a very old tree.²⁶ The magnetized points can be left either in a magnetized state, which represents “1,” or a demagnetized state, which represents “0.”²⁷ Whenever a user enters a command that requires the computer to access data stored on the hard drive or write data onto the hard drive, the platters spin and the magnetic heads are directed over that portion of the hard drive where the particular information is stored. As the magnetic heads pass over the magnetized points on the platters, they generate 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 drive into discrete subparts known as “clusters” or “allocation units.”²⁹ Different operating systems use clusters of different sizes,³⁰ typical cluster sizes might be four kilobytes or thirty-two kilobytes. A cluster is like a filing cabinet of a particular size placed in a storage warehouse. Just as a filing cabinet might store particular items in a particular place in the warehouse, the operating system might use a cluster to store a particular computer file in a particular place on the hard drive. The operating system keeps a list of where the different files are located on the

²⁴ This coding is known as the American Standard Code for Information Interchange (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 two to the thirtieth power bytes, which is about 1.073 billion bytes. See E. GARRISON WALTERS, *THE ESSENTIAL GUIDE TO COMPUTING* 12–13 (2001); MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY 492 (10th ed. 1996) (defining “gigabyte” as “1,073,741,824 bytes”).

²⁶ See KEOGH, *supra* note 23, at 144, 152–53; Craig Ball, *Computer Forensics for Lawyers Who Can’t Set the Clock on Their VCR*, in 6 ON FORENSICS 4, 9 (2005), available at http://www.craigball.com/cf_vcr.pdf.

²⁷ See KEOGH, *supra* note 23, at 141.

²⁸ See *id.* at 141–42, 152–53.

²⁹ PETER STEPHENSON, *INVESTIGATING COMPUTER-RELATED CRIME* 99–100 (2000); NELSON ET AL., *supra* note 19, at 80.

³⁰ See KEOGH, *supra* note 23, at 147.

hard drive; this list is known as the File Allocation Table or Master File Table (MFT), depending on the operating system.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 correct cluster.³²

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 Merely observing a room does not constitute a 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 visually observe the zeros and ones, and he does not physically move anything inside it. Retrieving information from a computer means entering commands that copy data from the magnetic discs, 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 home and computer searches concerns ownership and control over the item searched. When a police officer searches a home, the home and property he searches typically belong 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 the 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 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

³¹ See Ball, *supra* note 26, at 23–25.

³² If a file is larger than the cluster size used by that operating system, the operating system assigns multiple clusters to that file. The operating system’s master list keeps the list of different clusters where parts of that file are stored, and when the file is accessed, the heads are 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 23, at 149.

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, 812 (1982).

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

³⁶ See NELSON ET AL., *supra* note 19, at 50–51.

³⁷ See *id.* at 51.

normal copy duplicates only the identified file, but the bitstream copy duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original.³⁸ Whereas casual users make copies of files when their machines are running, analysts generally create bitstream copies using special software after the computer has been powered down.³⁹ The bitstream copy can then be saved as a “read only” file so that analysis of the copy will not alter it.

The accuracy of the bitstream copy often is confirmed using something called 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 determine whether two files are identical.⁴¹ If two nonidentical files are inputted into the hash program, the computer will output different results.⁴² If the two identical files are inputted, however, the hash function will generate identical output. Forensic analysts can use these principles to confirm that the original hard drive and the bitstream copies are identical.

The fact that computer searches generally occur on government property rather than the suspect’s raises important legal questions. What is the legal significance of generating the bitstream copy? Does that “seize” the original data, and, if so, is the seizure reasonable? How does the Fourth Amendment apply to analysis of copied data stored on a government computer? Does the retrieval of evidence from a copy stored on a government computer constitute a search? Or can the government search its copy of data without 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 their 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. They can destroy evidence and usually know if it has been destroyed. Computers can only store data, but the amount of data is staggering.

³⁸ See *id.* at 50.

³⁹ Interview with Mark Pollitt, former Dir., Reg’l Computer Forensic Lab. Program, in Wash., D.C. (Aug. 1, 2005).

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.* at 1234.

Computer hard drives sold in 2005 generally have storage capacities of about eighty gigabytes, roughly equivalent to forty million pages of text — about the amount of information contained in the books on one floor of a typical academic library. These figures will soon be outdated, as computer storage capacities tend to double about every two years.⁴³ At this rate, a new computer purchased in 2015 will store about twenty *trillion* zeros and ones.⁴⁴ 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 can often recover deleted files from a hard drive.⁴⁵ 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. Rather, most operating systems merely go to the Master File Table and mark that particular file’s clusters available for future use by other files. If the operating system does not reuse that cluster for another file by the time the computer is analyzed, the file marked for deletion will remain undisturbed. Even if another file is assigned to that cluster, a tremendous amount of data often can be recovered from the hard drive’s “slack space,” space within a cluster left temporarily unused.⁴⁶ It can be accessed by an analyst just like any other file.

Computer operating systems and programs also generate and store a wealth of information about how the computer and its contents have been used. As more programs are used, that information, called metadata, 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.⁴⁷

⁴³ See Kerr, *supra* note 3, at 302.

⁴⁴ I reached this estimate by multiplying 640 billion (the storage capacity of an eighty-gigabyte hard drive) by thirty-two, or two to the fifth power.

⁴⁵ See, e.g., United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).

⁴⁶ KEOGH, *supra* note 23, 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 contains unused space. Just as a filing cabinet reserved for a particular topic may be only partially filled, the cluster may be only partially occupied by its associated file. See Ball, *supra* note 26, at 26–28.

⁴⁷ Newer versions of Windows contain a New Technology File System (NTFS) log file, which 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 which users have access rights to them. NELSON ET AL., *supra* note 19, at 89–91. The MFT also stores the “MAC times” — when each file was Modified, Accessed, and Created — associated with each file. Bob Sheldon, *Forensic Analysis of Windows Systems*, in HANDBOOK OF COMPUTER CRIME INVESTIGATION 133, 134–37 (Eoghan Casey

Common word processing programs such as WordPerfect and Microsoft Word generate temporary files that permit analysts to reconstruct the development of a file.⁴⁸ Word processing documents can also store data about who created the file, as well as the history of the file.⁴⁹ Similarly, 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 the websites users have visited in recent weeks; users may use this history to retrace their steps or find webpages they previously visited. Some of this information may be very specific; for example, the address produced by an Internet search engine query generally includes the actual search terms the user entered.⁵⁰

The storage practices of computers prompt an important legal question: how can Fourth Amendment rules limit and regulate the scope of computer searches? The Fourth Amendment was created to abolish general warrants and require narrow searches. Can the rules that limit physical searches also apply to computer searches, or are new rules needed?

D. The Retrieval Mechanism: Physical vs. Logical

The fourth difference between home searches and computer searches concerns the techniques for finding evidence and the invasiveness of routine searches. Executing a physical search of a home generally requires assembling and training a search team. Police officers look from room to room for the evidence sought in the warrant. If the evidence sought is large, the police will limit their search accordingly: if they are looking for a stolen car, for example, they can't look inside a suitcase to find it.⁵¹ The police may conduct unusually thorough searches in particularly important cases, but such searches are costly and relatively rare. After the police have searched the space for the item sought, the search is done, and the police will leave.

Computer searches tend to require fewer people but more time. According to Mark Pollitt, former Director of the FBI's Regional Computer Forensic Laboratory Program, analysis of a computer hard

ed., 2002). MAC times are often important for determining when a particular file was created, or for helping establish whether it was tampered with. *See id.* at 134-36. 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* STEPHENSON, *supra* note 29, at 101-02; Ball, *supra* note 26, at 32-33.

⁴⁸ *See* Ball, *supra* note 26, at 33-34, 36-37.

⁴⁹ *See id.* at 36-37.

⁵⁰ For example, if a user enters a search for "assassinate & 'how to dispose of a body'" into the Google search engine, the URL for Google's report will be: <http://www.google.com/search?hl=en&q=%22assassinate%22+%26+%22how+to+dispose+of+a+body%22&btnG=Search>.

⁵¹ *See* United States v. Ross, 456 U.S. 798, 824 (1982).

drive takes as much time as the analyst has to give it.⁵² 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.⁵³ For an analyst, determining which approach to take usually requires consultation with both the warrant and the case agent. The forensic analyst ordinarily needs to know not only what kinds of searches the warrant permits as a matter of law, but also the type and amount of evidence needed as a practical matter to prove the government's case in court.⁵⁴

In contrast to physical searches, digital evidence searches generally occur at both a "logical" or "virtual" level and a "physical" level. The distinction between physical searches and logical searches is fundamental in computer forensics: while a logical search is based on the file systems found on the hard drive as presented by the operating system,⁵⁵ a physical search identifies and recovers data across the entire physical drive without regard to the file system.⁵⁶ Because of the need to conduct both physical and logical searches, the computer search process tends to be more labor intensive and thorough than the physical search of a home. Consider a search for a picture file believed to be evidence of a crime. An examiner might begin by conducting a logical search of the hard drive for files with extensions known to be used for image files, such as ".jpg."⁵⁷ 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 generally facilitates the latter with a simple command. For example, the current version of the EnCase forensic software has a feature called "Gallery View."⁵⁸ If an analyst selects a hard drive or folder to be searched and then clicks the "Gallery" button, the software looks for

⁵² Interview with Mark Pollitt, *supra* note 39.

⁵³ *Id.*

⁵⁴ *Id.* For example, in a child pornography case, the analyst may only need to find a certain number of images. Although it would be possible to spend weeks finding every single recoverable image stored on the hard drive, it would not advance the easily proven case.

⁵⁵ See KEOGH, *supra* note 23, at 144-46.

⁵⁶ See NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 15-16 (2004).

⁵⁷ The ".jpg" extension is used for image files created through a common compression algorithm, developed by the Joint Photographic Experts Group (JPEG), that allows pictures to be stored in a relatively small amount of space.

⁵⁸ See GUIDANCE SOFTWARE, ENCASE FORENSIC EDITION USER MANUAL 23 (Guidance Software EnCase Demo Disk CD-ROM, 4th version 2004).

all files ending with a picture file extension and automatically presents thumbnails of those files to the user.⁵⁹

This procedure sounds easy, but ordinarily does 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 with an extension common to a different kind of file, such as “.doc” or “.wpd.”⁶⁰ A search for picture files based on the logical file extensions will no longer locate the file. Instead, the analyst will have to conduct a search at a physical instead of logical level. Software can locate 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.⁶¹ The file header remains unchanged regardless of the extension placed on the file, allowing a physical search to uncover picture files that a logical search would not locate. In addition, file header characteristics can be located in slack space or in partially deleted files, allowing a skilled analyst to reconstruct the file and recover the associated picture.⁶² 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.⁶³

A search for text files resembles 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 and physical level.⁶⁴ Exact search protocols are difficult to settle *ex ante*; good forensic analysis is an art more than a science. To find a specific type of file believed to be stored in a particular location or generated by a particular program, an analyst might begin by looking first at that location or program. He might run 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 particular files, but more broadly throughout the entire hard drive. Searches also can be run with a predetermined 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

⁵⁹ *See id.*

⁶⁰ *See* NELSON ET AL., *supra* note 19, at 417, 490–93.

⁶¹ *See id.* at 493.

⁶² *See id.* at 493–517.

⁶³ Interview with Mark Pollitt, *supra* note 39.

⁶⁴ NELSON ET AL., *supra* note 19, at 380–85.

of “book-making” or “bkmaking.” If the error rate is set at fifty percent, however, the software will note any word that contains five or more of the ten letters in the word.⁶⁵

Analysts can also locate specific images, files, and applications by using the one way hash function mentioned earlier. The National Drug Intelligence Center has calculated and collected common hash values for nearly every known application and operating system file and for many images of child pornography in a database called the Hashkeeper.⁶⁶ Many forensic analysts also compile their own databases of hashes known to be associated with specific types of files. If there is a match between the hash of a known file in a database and a file located in the computer being searched, an analyst can be confident that he has identified a particular file without actually opening or looking at it. Once the analyst has located a file, he can record information about the file retained by the operating system, such as MAC times,⁶⁷ and the folder in which it was found.

Once again, it is not always this easy. Files can be scrambled into ciphertext.⁶⁸ Encrypted files cannot be read at all; they appear as mere gibberish to forensic tools and cannot provide evidence for law enforcement. When this is the case, a forensic analyst generally must attempt either to locate or guess the encryption “key” (usually a long string of numbers) to decrypt the files, or else find the “passkey” (usually a password) that can first decrypt the key and then allow the files to be decrypted.⁶⁹ In some cases, the key or passkey may be located somewhere in the hard drive. In other cases, the analyst must try to guess the key using special software.⁷⁰ Sometimes this will work, allowing the files to be decrypted,⁷¹ but this process can take weeks and often is not successful at all.

The differences between computer searches and traditional physical searches raise difficult questions about the rules that should govern

⁶⁵ This example is taken from *id.* at 384–85. Many computer forensics programs have special tools to simplify searches in specific contexts. For example, EnCase has a feature that tabulates the MAC times of all 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 during which the computer was heavily used. The software arranges the files by date, greatly simplifying the work of the analyst.

⁶⁶ See *id.* at 237.

⁶⁷ See Sheldon, *supra* note 47, at 134–37.

⁶⁸ See Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 530 (2005).

⁶⁹ See *id.*

⁷⁰ See ELEC. FRONTIER FOUND., *CRACKING DES: SECRETS OF ENCRYPTION RESEARCH, WIRETAP POLITICS & CHIP DESIGN* (1998).

⁷¹ See, e.g., *United States v. Scarfo*, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

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 they are more of an art than a science. The search can require a very time-consuming and invasive process 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 suspect'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 reduction stage, the investigator begins with an image of the hard drive and attempts to locate particular evidence it may contain. To borrow a physical metaphor, data acquisition refers to collecting the hay, and data reduction involves looking through the haystack for the needle.

This Part considers two aspects of how the Fourth Amendment applies to the data acquisition stage of the computer forensics process: 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, namely whether or when a search or seizure has occurred. Searches and seizures are presumptively unreasonable, and therefore unconstitutional, unless a warrant has been obtained or an exception to the warrant requirement applies.⁷² In contrast, conduct that does not constitute a search or seizure remains unregulated by the Fourth Amendment.

This Part proposes that the rules for looking through a computer should be governed by the Fourth Amendment's prohibitions on searches, and specifically by 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 observable retrieval of information stored on a computer hard drive, no matter how minor, should be

⁷² See *Payton v. New York*, 445 U.S. 573, 586 (1980).

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 ignores 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 a warehouse to zones of human observation. Under this approach, agents are generally prohibited from retrieving evidence from computers unless they have a warrant or an exception to the warrant requirement applies. Further, in the case of a search by a private actor, government agents may view only the 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 remove the original data, 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 and instead use the Fourth Amendment to impose limitations on creating bitstream copies of computer storage devices. There are multiple ways to adjust existing doctrine to achieve such a result, and the precise path may not matter a great deal. On balance, however, the best route is to retain the existing definition of seizures and to regulate imaging based on how it interferes with the computer that is imaged. In addition, 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, these guidelines would place Fourth Amendment limits on both 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.⁷³ Or perhaps a private party finds evidence of a crime on a computer and turns it over to the police for further investigation.⁷⁴ In either case, the investigator may want to look through a few files on the computer to see what information it contains. This

⁷³ See, e.g., *United States v. Turner*, 169 F.3d 84, 86 (1st Cir. 1999).

⁷⁴ See, e.g., *United States v. Runyan*, 275 F.3d 449, 453 (5th Cir. 2001).

section considers the Fourth Amendment rules that should regulate such scenarios.

The Supreme Court has defined a Fourth Amendment “search” as government action that violates an individual’s “reasonable” or “legitimate” expectation of privacy.⁷⁵ In the context of physical spaces, searches generally refer to intrusions into private areas. A house is searched when a government agent enters it; a package is searched when a government agent opens it.⁷⁶ Individuals ordinarily have a reasonable expectation of privacy in their homes and packages, and the act of breaking the seal between public space and the private home or package triggers a search. With respect to the home, physical entry is the most common (although not the only⁷⁷) means of breaking down the barrier between public and private. It exposes the inside of the home to observation that is impossible from the 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. Just as an individual generally has a reasonable expectation of privacy in his home and his packages, so too should he have a reasonable expectation of privacy in the contents of his personal hard drive. A suspect’s hard drive is his private property, much like other sealed containers, and the same rules should apply. Unusual circumstances may lead to a different result,⁷⁸ but the starting point for applying the Fourth Amendment to a computer hard drive is clear and generally uncontroversial: the Fourth Amendment applies to computer storage devices just as it does to any other private property.⁷⁹

⁷⁵ *Smith v. Maryland*, 442 U.S. 735, 739–40 (1979) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

⁷⁶ *See, e.g., Wilson v. Layne*, 526 U.S. 603, 610 (1999) (search of a home); *United States v. Ross*, 456 U.S. 798, 822–23 (1982) (search of a package).

⁷⁷ *See, e.g., Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding that use of a thermal imaging device from outside the home constitutes a search of the home because it permits investigators to observe details about the inside of the home previously unknowable without physical entry).

⁷⁸ *See, e.g., United States v. Caymen*, 404 F.3d 1196, 1200–01 (9th Cir. 2005) (no reasonable expectation of privacy in computer obtained by fraud); *United States v. Wong*, 334 F.3d 831, 839 (9th Cir. 2003) (no reasonable expectation of privacy in stolen computer); *United States v. Lyons*, 992 F.2d 1029, 1031–32 (10th Cir. 1993) (no showing of actual, subjective expectation of privacy in stolen computer).

⁷⁹ *See United States v. Blas*, No. 90-CR-162, 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 . . .”); *see also Runyan*, 275 F.3d at 458 (reasonable expectation of privacy in computer disks); *United States v. Reyes*, 922 F. Supp. 818, 832–33 (S.D.N.Y. 1996) (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, the fact that the Fourth Amendment applies equally to computer storage devices has been implicit in decisions that focused on other

Cases applying the Fourth Amendment to containers also provide a natural starting point for identifying what it means to “search” a computer. “Containers” are a well-defined category within Fourth Amendment law. The Supreme Court has developed a set of rules that applies equally to all containers, protecting “a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf” the same as “the sophisticated executive with the locked attaché case.”⁸⁰ The foundational premise of the container cases is that opening a 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.⁸¹

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.⁸² This is a good start, and likely an uncontroversial one. Accessing information from a computer breaks the seal between public and private, much like entering a home or opening a package. For doctrinal purposes, this is a 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 important mostly for purposes of civil liability: if the general process of accessing information on a computer can constitute a search, at exactly what stage does the search occur — when the hard drive heads read the data from the drive, when the computer collects the data, when the analyst can see the data, or at some other point?⁸³ The second question concerns the zone or scope of a search: when a user retrieves data from a hard drive, how much has been

questions. *See, e.g.*, *United States v. Carey*, 172 F.3d 1268, 1273–76 (10th Cir. 1999) (plain view and warrant case); *United States v. Upham*, 168 F.3d 532, 536–37 (1st Cir. 1999) (warrant case).

This discussion assumes that the computer storage device 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.

⁸⁰ *Ross*, 456 U.S. at 822.

⁸¹ *See id.* at 822–23.

⁸² *See Henderson*, *supra* note 68, at 530.

⁸³ This question primarily affects civil liability because the government must observe information to use it in a criminal case. If the government attempts 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 at which 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.

searched? This is an essential question because if a particular government action constitutes a search of a given zone, then the government agent does not need any additional justification to examine and analyze anything within that zone. The zone determines whether a search of *A* allows a subsequent search of *B*.

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 hard drive that contains the relevant data, inducing a current in a wire that carries away the signal.⁸⁴ This generates a copy of the data, and the computer sends the copy to its central processing unit. The copy may be stored temporarily in various types of memory, or it may be copied to another storage device, and it is ultimately processed by the software running on the computer. The output that a user sees on his screen 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 data stored on a hard drive — copying, collecting, and processing the 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 it 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 supports it.

First, focusing on the exposure of data most accurately transfers our physical world notions of searches to the context of computers. Entering a house is a search of physical space because it exposes to human observation the otherwise hidden interior of the house.⁸⁵ In the computer context, there is no need to focus the "search" inquiry on a physical action like entry; the law can look directly to exposure. The exposure-based approach focuses doctrinal attention on the key question from the perspectives 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 Amend-

⁸⁴ See KEOGH, *supra* note 23, at 141–42.

⁸⁵ *Cf.* *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

ment as a barrier to the retrieval of information from nonobservable form to observable form.

Second, the exposure-based approach reinforces the traditional Fourth Amendment concern with limiting the scope of searches.⁸⁶ Defining searches in terms of 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 is one that exposes less. Other approaches de-link the measured scope from the actual level of intrusiveness of the government conduct. For example, imagine if a search occurred whenever data 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 “assassination” anywhere on a hard drive may be broad at a physical level — the entire hard drive must be scanned — but its invasion of privacy is fairly slight. 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 amounts 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 traditional Fourth Amendment concerns about limiting the scope of searches.

Third, the exposure-based approach proves much easier to administer than the alternatives. It is far easier for humans to control and understand exposure than to control and understand 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 such technicalities would be hard to impose *ex ante* and difficult to apply *ex post*. Analysts would need to be aware of exactly when the operating system was directing the computer to read from particular places on a hard drive, and judges would need to understand these highly technical and contingent details as well. Many cases would require the consultation of technical experts to try to reconstruct exactly what bits from the hard drive were copied or processed, even if they were captured for only a nanosecond and no record of them was 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.⁸⁷

⁸⁶ See *infra* p. 565.

⁸⁷ 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).

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*.⁸⁸ The defendant in *Karo* received what he thought were cans of ether needed to extract cocaine as part of a narcotics conspiracy.⁸⁹ 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.⁹⁰ The Tenth Circuit held that transferring the transmitter to Karo violated his Fourth Amendment rights because the transmitter had the potential to reveal invasive information.⁹¹ 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.⁹²

This information-focused approach is echoed by *Kyllo v. United States*,⁹³ in which federal agents used a thermal imaging device to pick up infrared radiation from the surface of a home. Because infrared radiation varies as a function of surface temperature, measurements of such radiation can be used to create an image of surface temperatures. The Court held that the display of “hi-tech measurement of emanations from a house”⁹⁴ to determine the temperature of the wall was a search.⁹⁵ 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 by a machine.⁹⁶ For the holding in *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 in *Kyllo* a search 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 com-

⁸⁸ 468 U.S. 705 (1984).

⁸⁹ *Id.* at 708.

⁹⁰ *Id.*

⁹¹ See *United States v. Karo*, 710 F.2d 1433, 1438 (10th Cir. 1983).

⁹² *Karo*, 468 U.S. at 712.

⁹³ 533 U.S. 27 (2001).

⁹⁴ *Id.* at 37 n.4.

⁹⁵ *Id.* at 40.

⁹⁶ See J.M. LLOYD, THERMAL IMAGING SYSTEMS 1–2 (1975).

puters strongly suggests that a search occurs when digital information is exposed to human observation, not when it is copied from a hard drive.⁹⁷

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. The zone of a search determines the extent to which a particular search in a space eliminates privacy protection elsewhere in that space. When particular data from a particular hard drive is displayed to a user, how much of the hard drive has been searched?

This inquiry is often overlooked in the case of physical searches, but it is quite important. The zone of a physical search is largely intuitive; it correlates neatly with what is hidden and what is exposed.⁹⁸ For example, if police enter a house, the entry is a search. But merely entering the house does not constitute a legal “search” of everything inside it. Under existing law, the opening of any closed containers inside the house constitutes a separate search.⁹⁹ The zone of the initial search includes open areas of the house, but does not extend to property in the house 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 contents of a virtual file, the physical storage device, or the exposed data. If the zone is a device, then opening it searches all of its contents. If the zone is a file, then that file is searched but the rest of the computer is unsearched. Finally, if the zone is the exposed data itself, then exposure of data leaves all unexposed information unsearched.

Existing case law reflects both virtual file and physical device approaches to defining 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*.¹⁰⁰ 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

⁹⁷ See *Brower v. County of Inyo*, 489 U.S. 593, 596 (1989).

⁹⁸ The precise zone of a search is critical only when the government’s authority to conduct a search extends to one zone but not to others. If the government’s authority to search covers multiple spaces — as with a search warrant, which ordinarily permits searching all of the zones in the place to be searched that can physically accommodate 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.

⁹⁹ See *United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978) (holding that a search of a footlocker violated the Fourth Amendment even though it was located in a room the police could have lawfully searched).

¹⁰⁰ 172 F.3d 1268 (10th Cir. 1999). For a similar approach, see *United States v. Barth*, 26 F. Supp. 2d 929, 936–37 (W.D. Tex. 1998).

child pornography.¹⁰¹ He subsequently opened a string of additional files containing child pornography. The court held that the first discovered image was admissible, but that the subsequently opened files were beyond the scope of the warrant.¹⁰² 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. A computer is like a container that stores thousands of individual containers in the form of discrete files.

The Fifth Circuit's decision in *United States v. Runyan*¹⁰³ offers an example of the physical device approach. 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.¹⁰⁴ 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 than the wife had seen. There was no record of what specific 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 entirety of the disks.¹⁰⁵ The container was the physical hard drive, and a search of some files in the container left it open to further inspection. According to the Fifth Circuit, any additional analysis of the disks merely "expanded" the prior search.¹⁰⁶ The fact that the police had opened different files did not matter, as the zone of the search was defined by the physical storage devices.¹⁰⁷

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 the information they contain. When assessing how the Fourth Amendment

¹⁰¹ See *Carey*, 172 F.3d at 1271.

¹⁰² *Id.* at 1273 & n.4.

¹⁰³ 275 F.3d 449 (5th Cir. 2001).

¹⁰⁴ See *id.* at 452-53.

¹⁰⁵ See *id.* at 464-65.

¹⁰⁶ *Id.* at 460 n.11.

¹⁰⁷ See also *United States v. Slanina*, 283 F.3d 670, 680 (5th Cir. 2002). An analogous issue was addressed but not resolved by the Supreme Court in *Waller v. United States*, 447 U.S. 649 (1980). In *Waller*, 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 film 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, modeling the film as a physical box, see *id.* at 663 (Blackmun J., dissenting); two Justices said no, modeling the film as the information it contained, see *id.* at 659 (Stevens, J., announcing the judgment of the Court); and three Justices either did not resolve the case on that ground, see *id.* at 660 (White, J., concurring in the judgment), or did not explain their rationale, see *id.* (Marshall, J., concurring in the judgment).

applies to the collection of information, courts should focus on that information rather than the physical storage device that happens to contain it. Using the physical box as the common denominator of a computer search would also lead to unpredictable, unstable, and even disturbing results. As computers contain more and more information over time, it becomes increasingly awkward to say that a second search through the contents of a computer simply examines the contents of the physical box in a more comprehensive manner than before.

This point is all the more clear in a networked world. 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. Furthermore, a single file on a network may actually be stored in several 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 storage device as the proper zone of a computer search, the next question is a subtle one: is the proper zone the virtual file or the exposed data? Existing cases tend to ignore this question because they mostly involve possession of digital images of child pornography, in which the contraband image is both the file contents and the exposed data. The distinction between files and data collapses in this context though in other cases the distinction will prove tremendously important. Imagine that an officer executing a search warrant comes across a computer that is up and running with the first page of a one hundred page document on the screen. The officer wants to view the other ninety-nine pages of the document to see if they reveal evidence of criminal activity. If 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 one hundred 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 exposed information as the common denominator. 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, much information stored on a computer does not appear in a file.¹⁰⁸ If the law is keyed to files,

¹⁰⁸ See *supra* pp. 542-43.

how can it apply to information not stored in a file? Second, this approach fits nicely with the exposure-based approach to searches. Once again, what matters is exposure to human observation. Third, virtual files are not robust concepts. Files are contingent creations assembled by operating systems and software. 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 from another analyst who double clicks on a second file to open it. In both cases, the analysts are exposing information not previously exposed. Both actions 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 normally 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 that may be justified by the warrant. Under the exposure standard, the same rule would apply to observing unexposed portions of large computer files. The exposure-based 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.¹⁰⁹ 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."¹¹⁰ 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 and therefore requires a warrant or an exception to the warrant requirement.

Existing doctrine, however, has suggested otherwise. Under *Arizona v. Hicks*,¹¹¹ merely copying information does not seize anything.¹¹² As a result, a choice exists between two basic approaches.

¹⁰⁹ See, e.g., Brenner & Frederiksen, *supra* note 1, at 111–12.

¹¹⁰ *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

¹¹¹ 480 U.S. 321 (1987).

¹¹² *Id.* at 324.

Under the first approach, the creation of a copy does not constitute a search or seizure. Under the second approach, some doctrinal hook is found to ensure that generating a bitstream copy does count as a search or seizure, either by rejecting *Hicks* in the context of digital evidence or through some other approach. On balance, I think that the better approach is the second one, but that courts should reach this result while retaining *Hicks*. Creating a bitstream copy should require a warrant or an exception because of the way it manipulates the machine, not because of the copy it generates. Finally, the Fourth Amendment rules that apply to originals should also apply to bitstream copies.

1. *Hicks and Other Precedents on Seizing Information.* — In *Hicks*, 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 its components. A quick call to headquarters confirmed a match between the serial numbers and stereo components stolen during an armed robbery.¹¹³ 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.¹¹⁴

Although reproducing the data generated a copy of it, the creation of a copy did not constitute a seizure.

Lower courts have followed this approach in cases involving photocopies and photographs. In *United States v. Thomas*,¹¹⁵ a package sent via UPS ripped open during sorting and revealed obscene materials inside it.¹¹⁶ UPS employees called the FBI, and an FBI agent made photocopies of the materials before resealing the package. The package was found to be undeliverable to both the addressee and the return address, and the FBI left the package with UPS.¹¹⁷ FBI agents then requested a warrant to seize the package and attached the photocopies of the pages to the affidavit.¹¹⁸ Thomas challenged the FBI’s conduct, claiming that the government had impermissibly seized the

¹¹³ *Id.* at 323–24.

¹¹⁴ *Id.* at 324 (citing *Maryland v. Macon*, 472 U.S. 463, 469 (1985)).

¹¹⁵ 613 F.2d 787 (10th Cir. 1980).

¹¹⁶ *Id.* at 789.

¹¹⁷ *Id.* at 793.

¹¹⁸ *Id.* at 790–91.

materials.¹¹⁹ The Tenth Circuit disagreed, noting that photocopying the items did not seize them: “The materials herein remained in UPS’s possession and their delivery was unaffected since they were undeliverable. The materials were searched but not seized.”¹²⁰ Similarly, in *Bills v. Aseltine*,¹²¹ police officers took photographs of a home during the execution of a warrant at the property. The homeowner sued the officers, alleging that taking the pictures had seized images of her home in a way not permitted by the warrant.¹²² The Sixth Circuit relied on *Hicks* and rejected the claim. The court concluded 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.”¹²³

One district court has applied the same rationale to the copying of computer files, albeit as an alternative holding in an unpublished opinion. In *United States v. Gorshkov*,¹²⁴ FBI agents accessed the Internet account of a suspect and downloaded his files without obtaining a warrant. Relying 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.”¹²⁵

Some authorities construing Rule 41 of the Federal Rules of Criminal Procedure are at odds with *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.¹²⁶ In a series of cases in the 1970s and 1980s, courts considered whether Rule 41 authorizes investigators to obtain information through the use of pen register devices and “sneak and peek” searches, even when no tangible evidence is seized.¹²⁷ Courts construed the Rule 41 power broadly, rejecting claims that such surveillance was impermissible. The courts’ opinions implicitly (and sometimes explicitly) indicated

¹¹⁹ *Id.* at 792.

¹²⁰ *Id.* at 793.

¹²¹ 958 F.2d 697 (6th Cir. 1992).

¹²² *See id.* at 707.

¹²³ *Id.* (quoting *Arizona v. Hicks*, 480 U.S. 321, 324 (1987)).

¹²⁴ No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

¹²⁵ *Id.* at *3. Another district court rejected the idea that making a bitstream copy of a suspect’s hard drive was a seizure of the entire hard drive, but the opinion is too cryptic to make much of the court’s conclusion. *See United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 48 (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).

¹²⁶ FED. R. CRIM. P. 41(b).

¹²⁷ *See, e.g., United States v. N.Y. Tel. Co.*, 434 U.S. 159 (1977) (pen register); *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986) (sneak and peek warrant).

that recording information “seized” it.¹²⁸ The close 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 considered a “seizure.” At the same time, the context 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 peculiar 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 precedential authority, *Hicks* and its progeny seem to outweigh the Rule 41 cases in defining seizures of information.

2. *Bitstream Copies and the Fourth Amendment.* — If *Hicks* dictates that generating a copy of information does not amount to a seizure, its application 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 obtain a perfect copy without depriving the owner of the original.¹²⁹ 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.¹³⁰ If generating a copy is neither a search nor a seizure, the police may be able to generate bitstream copies without Fourth Amendment limits.

This is a troublesome result. Permitting the government to make and retain copies of our private electronic files seems inconsistent with our traditions. The idea that the government could freely generate copies of our hard drives and indefinitely retain them in government storage seems too Orwellian — and downright creepy — to be embraced as a Fourth Amendment rule. Granted, the implications of such a rule might be softened 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 examine the images without a warrant. The difficulty with this rule is that bitstream copies are stored by the government on government machines.

¹²⁸ See, e.g., *N.Y. Tel.*, 434 U.S. at 169 (holding that Rule 41 “is broad enough to encompass a ‘search’ designed to ascertain the use which is being 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 [and that the] intangible property to be ‘seized’ was information regarding the ‘status’” of the place to be searched).

¹²⁹ Cf. Mark A. Lemley, *Ex Ante Versus Ex Post Justifications for Intellectual Property*, 71 U. CHI. L. REV. 129, 143 (2004) (discussing how copying resources spreads ideas and increases information).

¹³⁰ Some small amount of metadata would be exposed in most cases, however, and that information would be considered the fruit of a “search.” See *supra* pp. 542–43.

As a result, it may be difficult or impossible to know whether investigators are complying with the rules. A suspect has no way of controlling access to or use of the copy.¹³¹

Courts could follow either of two alternative strategies to avoid such a result and regulate the imaging process under the Fourth Amendment. First, courts could depart from *Hicks* in cases involving 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.¹³² Second, courts could regulate imaging by focusing on the interference and manipulation of the machine rather than the duplication itself. Because imaging generally requires commandeering the computer and disabling access to the computer for a matter of hours,¹³³ the computer ordinarily is “seized” during this time under the existing definition of a “seizure.”¹³⁴ As a result, even the act of connecting a cable to an input/output port may be a Fourth Amendment search or seizure. Further, some circuit courts have held that inserting a key into a lock without opening the door constitutes a search.¹³⁵ Although the analogy between connecting a cable and inserting a key is not exact, these cases at least suggest room in existing doctrine for the view that the connection of a cable for data transmission constitutes a search.

As a practical matter, it probably makes little difference which path is chosen.¹³⁶ Either one would require a valid warrant or an exception to the warrant requirement before the government could image a person’s computer. On balance, however, I think the latter approach is preferable. 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

¹³¹ Thanks to Eugene Volokh for this point.

¹³² See Brenner & Frederiksen, *supra* note 1, at 111–12.

¹³³ Interview with Mark Pollitt, *supra* note 39.

¹³⁴ See *Illinois v. McArthur*, 531 U.S. 326, 329–30 (2001) (holding that blocking the defendant from entering his house while the police obtained a search warrant is a temporary seizure); see also Brenner & Frederiksen, *supra* note 1, at 113.

¹³⁵ See *United States v. Concepcion*, 942 F.2d 1170, 1173 (7th Cir. 1991) (Easterbrook, J.); *United States v. Portillo-Reyes*, 529 F.2d 844, 848 (9th Cir. 1975). In these cases, the police had a key in their possession and inserted the key into a lock in an attempt to determine ownership. Other courts have taken a different approach. See *United States v. Lyons*, 898 F.2d 210, 213 (1st Cir. 1990) (“We conclude that this course of investigation [of inserting a key into a lock] did not constitute a search . . . or at least, not an unreasonable search protected by the Fourth Amendment.” (citation omitted)); *United States v. DeBardeleben*, 740 F.2d 440, 443–45 (6th Cir. 1984).

¹³⁶ One possible difference concerns whether the Fourth Amendment regulates creating a copy of the copy. If duplication constitutes a seizure, then copying the copy would implicate the Fourth Amendment as well; in contrast, if the key question is interference with the owner’s property, creating another reproduction likely would not implicate the Fourth Amendment.

necessarily generates a copy of that data, if only for internal purposes. If copying computer data seizes it, then using a computer would seem to trigger constant seizing. There may seem to be an intuitive difference between generating a copy of data incidentally as a byproduct of normal computer usage and generating a copy for the purpose of creating a bitstream image, but it is difficult to turn that intuition into a legal rule.¹³⁷ 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 consider the duration of a seizure when determining its reasonableness.¹³⁸ 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, how long is the data 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.¹³⁹

3. *Copies vs. 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 property. Under the former approach, the restrictions on searching the original carry over to searching the copy; under the latter, the government can search the copy without restriction. I contend that the better choice is to treat copies in the same way as originals. Courts should apply identical rules regardless of whether the data analyzed is the original version or a government-generated copy. This is an important point given that

¹³⁷ One approach could be to focus on the officer's intent. Perhaps the intentional creation of a copy should be treated as different from the incidental creation of a copy. *Cf.* *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.” (quoting *Byars v. United States*, 273 U.S. 28, 33 (1927))). At the same time, this approach 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.”).

¹³⁸ *See, e.g., United States v. Place*, 462 U.S. 696, 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].”).

¹³⁹ *See supra* p. 542. Finally, a departure 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?

forensic analysts generally make a bitstream copy of files and analyze the copy instead of the original.¹⁴⁰ Under my approach, courts should find that the creation 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 dealing with the treatment of copies of seized property 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 Holmes¹⁴¹ and Judge Learned Hand¹⁴² forbade government use of document copies when the originals had been illegally seized. Although these cases may be read as extending the same protections to copies as to originals, it is probably fairer to view them as antecedents to the modern “fruit of the poisonous tree” doctrine.¹⁴³ More recently, federal appellate cases involving motions to return photocopies of seized documents have been brought under Rule 41 of the Federal Rules of Criminal Procedure.¹⁴⁴ These cases mostly involve the exercise of equitable powers to return property, however, and not the Fourth Amendment.¹⁴⁵ A possible exception is *Vaughn v. Baldwin*,¹⁴⁶ 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 search the originals. The reasoning of *Vaughn* is cursory and unclear, however, rendering it of little help in discerning the role of the Fourth Amendment.¹⁴⁷

The Fourth Amendment rules governing searches of copies may remain uncertain because copying has long required human exposure and involvement. When copying involves human observation, it will usually be clear that examining copied information is not a search. Recall *Hicks*, in which a police officer copied serial numbers from stolen audio equipment. Having just recorded the information himself by

¹⁴⁰ See *supra* p. 540.

¹⁴¹ See *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 391–92 (1920) (Holmes, J.).

¹⁴² See *United States v. Kraus*, 270 F. 578, 581 (S.D.N.Y. 1921) (Hand, J.).

¹⁴³ See *Wong Sun v. United States*, 371 U.S. 471, 484 (1963) (holding that evidence procured as the “fruit” of an unlawful search is inadmissible).

¹⁴⁴ FED. R. CRIM. P. 41(e).

¹⁴⁵ See, e.g., *Sovereign News Co. v. United States*, 690 F.2d 569, 571 (6th Cir. 1982); *Mason v. Pulliam*, 557 F.2d 426, 429 (5th Cir. 1977).

¹⁴⁶ 950 F.2d 331 (6th Cir. 1991).

¹⁴⁷ Judge Nelson’s opinion focused on the government’s decision to wait months before copying the documents and its subsequent refusal to return the documents after consent was revoked. Judge Nelson found this conduct “unreasonable” and therefore unconstitutional. See *id.* at 333–34. This reasoning sheds little light on whether looking through the copies in a timely manner constitutes a search.

hand, it seems obvious that the officer can look again at the piece of paper without violating the Fourth Amendment.¹⁴⁸ 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 case law does not provide an answer, existing practice may do so. Generating and analyzing bitstream copies are routine parts of the forensics process, and no court has ever considered searches of copies as different from searches of originals. In the handful of cases in which 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 that this fact made any difference.¹⁴⁹ From a practical perspective, this is the best approach. All computer 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 central processor. More broadly, computers work by copying and recopying information from one section of the machine 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-based approach to 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 the 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.

¹⁴⁸ See *supra* pp. 557–58.

¹⁴⁹ See, e.g., *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 48–53 (D. Conn. 2002) (search of a mirror image of a hard drive); *United States v. Gallo*, 55 M.J. 418, 422–23 (C.A.A.F. 2001) (same); *Commonwealth v. Ellis*, 10 Mass. L. Rptr. 429, 435–40 (Mass. Super. Ct. 1999) (same).

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. During this phase, investigators search through an image of the suspect'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. But many questions about the scope of the warrant remain. What steps can the police take to find the evidence named in the warrant? What kinds of searches pursuant to a warrant are "reasonable," and what kinds are "unreasonable"? Which rules should regulate *ex ante* what steps the police can take, and which rules should regulate *ex post* the admissibility of the files they discover?

The overarching challenge is finding a way to regulate the invasiveness of computer searches pursuant to a warrant. 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 thing to be seized.¹⁵⁰ In the physical world, this requirement imposes a serious restriction on police conduct, as it regulates where the police can go and which tangible objects they can seize. The police can only go to 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.¹⁵¹

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 variety of reasons, computer technologies may allow warrants that are particular on their face to become general warrants in practice. Computers tend to play an ever greater role in our lives as computer technologies advance, as they are likely to record and store increasingly detailed pictures of our daily experience. At the same time, the particularity requirement does less and less work as the storage capacity of computer devices gets greater and greater.¹⁵² Even if the property 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 trends sug-

¹⁵⁰ U.S. CONST. amend. IV.

¹⁵¹ See *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.[]'" (quoting *United States v. Ross*, 456 U.S. 798, 824 (1982))).

¹⁵² See *Kerr*, *supra* note 3, at 302–03.

gest that as time passes, rules created to prevent general searches for physical evidence may result in the equivalent of general searches for digital evidence. A warrant to seize and search a computer may justify a highly invasive search that uncovers a great deal of information beyond the scope of the warrant.

Two basic strategies exist for regulating and narrowing the invasiveness of computer searches to restore the function of preexisting rules for the digital 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 forensics process. According to this approach, computer warrants should state not only *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 the equivalent of general warrants. In contrast, 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, when the government seeks to introduce this evidence at trial.

This Part addresses both approaches. It begins by explaining why the environment of digital evidence raises special concerns about general searches. It then contends that *ex ante* restrictions are an inappropriate response 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 even in 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 pretextual search designed to discover the evidence subsequently obtained. 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 gives them a very valuable tool to gather evidence and fight crime. It provides an extra mechanism to protect public safety, with no added risk to privacy; after all, the police have already conducted the search.¹⁵³ Denying the police the use of powerful evidence if they come across it legitimately during a search seems to punish them for good police work and good fortune.¹⁵⁴

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 pretextual searches and fishing expeditions.¹⁵⁵ When combined with the considerable breadth of many low-level offenses,¹⁵⁶ the ability to engage in pretextual searches may permit the police to target unpopular or politically powerless persons or groups for heightened scrutiny. Probable cause that a particular person has committed a low-level offense may be relatively easy to establish, giving the police tremendous power to execute invasive searches upon a 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.¹⁵⁷ While courts generally will not scrutinize subjective intent to assess the validity of Fourth Amendment searches and seizures,¹⁵⁸ the fear that legal rules may enable pretextual or general searches still remains a key principle driving Fourth Amendment doctrine.¹⁵⁹

The plain view doctrine is the legal rule that balances the competing concerns of protecting public safety and preventing misuse of government power in this context. In its current form, the plain view doctrine permits the police to seize evidence discovered during a valid search if the incriminating nature of the item to be seized is immediately apparent.¹⁶⁰ The fairly broad scope of the doctrine reflects a judgment that the dynamics of physical evidence collection render the

¹⁵³ See *Coolidge v. New Hampshire*, 403 U.S. 443, 467–68 (1971) (plurality opinion).

¹⁵⁴ 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).

¹⁵⁵ See *Coolidge*, 403 U.S. at 466–67 (plurality opinion).

¹⁵⁶ William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 512–18 (2001).

¹⁵⁷ See LASSON, *supra* note 6, at 94–95.

¹⁵⁸ See *Whren v. United States*, 517 U.S. 806, 813 (1996).

¹⁵⁹ See *Horton v. California*, 496 U.S. 128, 138–40 (1990) (rejecting a subjective intent test for the plain view exception but recognizing that the possibility of officers using plain view to execute pretextual searches is a legitimate Fourth Amendment concern).

¹⁶⁰ See *id.* at 136–37.

risk of pretextual and dragnet searches relatively low. *Horton v. California*¹⁶¹ provides a useful illustration. In *Horton*, the Supreme Court held that the plain view exception justifies a search even if the officer had the subjective intent to execute a pretextual search.¹⁶² 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.¹⁶³ Second, the fact that police could only look in places and containers large enough to contain the specific physical evidence sought necessarily limited the scope of warrantless searches.¹⁶⁴

B. Reasonableness and Digital Evidence Collection

The realities of the computer forensics process present a very different dynamic, suggesting 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.¹⁶⁵ The particularity requirement reflects a physical concern: the thinking is that the law can limit searches by confining where in the physical world the police search and by naming the object of the search. Searching 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. This virtual world is growing rapidly, with the storage capacity of new computer hard drives tending to double every two years.¹⁶⁶ In the case of warrantless searches, there is no *ex ante* determination of the particularities of the search, and because digital evidence can be

¹⁶¹ 496 U.S. 128.

¹⁶² *Id.* at 138–39.

¹⁶³ *Id.* 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” (second alteration in original) (quoting U.S. CONST. amend. IV)).

¹⁶⁴ See *id.* at 140–41 (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)).

¹⁶⁵ Kerr, *supra* note 3, 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.”).

¹⁶⁶ *Id.* at 302.

located anywhere on a hard drive, the police can no longer rule out particular places based on the characteristics of the evidence sought.

Second, computers are playing an ever greater role in daily life and are 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 more. As computers become involved in more aspects of our lives, they record increasingly diverse information. Each new software application means another aspect of our lives monitored and recorded by our computers. As Part I demonstrates, 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 perform more functions and preserve more data, we may eventually approach a world in which a considerable chunk of our lives is recorded and stored in perpetuity in our computers. These details may end up stored inside our machines in a way that can be reconstructed later by a forensic analyst with remarkable 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 of many types of searches, including searches of homes. Few searches feature anything approaching 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. The analyst can comb through the computer for months; the only limit is the time the analyst has to give to 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 inconvenience of invasive searches, making such searches the norm rather than the exception.

To some extent, the invasiveness of computer searches in the future will depend on the development of forensic technology, the path of which is uncertain. Computer forensics programs evolve every year, and their features change on a regular basis. Computer searches may be invasive today, but may be less invasive 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 de-

scribed in the warrant, and the tool will find 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 pretextual and dragnet searches will depend at least in part on which future unfolds.

Despite this uncertainty, it seems likely that computer searches will continue to be highly invasive in the future. Perfect Tool sounds wonderful in theory, but it is likely impossible in practice; new technologies always produce countertechnologies designed to thwart them. Investigators and sophisticated wrongdoers inevitably play a cat-and-mouse game in which suspects try to hide evidence and forensic analysts try to find it. Given this dynamic, the possibility of ever completely ruling out a particular search appears remote. 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 very rare uses of such counterstrategies would trigger a legitimate law enforcement need for General Tool in many cases; investigators generally will not know *ex ante* whether a computer's owner took countermeasures to thwart government searches.¹⁶⁷ In this environment, Perfect Tool may not be possible. It therefore seems likely that tools closer to General Tool will be the norm in the future. Although tools that offer the promise of Perfect Tool may be used, a need will always exist for something more like General Tool.

For all of these reasons, the balance struck by existing law between protections for suspects and the need for crime control may need to be rethought in the future for the case of digital evidence. Many computers may contain a wealth of evidence of low-level crimes, and probable cause to believe a person has engaged in a minor offense may justify an exhaustive search of his hard drive that will expose a great deal to government observation. The existing plain view exception remains rooted in the contingent dynamics of physical evidence collection, which indicates a need to rethink the exception given the very different dynamics of digital evidence collection. The overall goal, however, should remain the same: the law should attempt to balance the threat of general searches against the public benefit of recovering additional

¹⁶⁷ *Cf.* *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (noting that investigators cannot rely on file suffixes to limit searches for computer files because they do not know if the computer's owner attempted to hide his files by changing the file suffixes).

evidence. The question is, what rules can best serve that balance in the context of the computer forensics process?

C. *Ex Ante* Restrictions for Computer Warrants

One response to the new dynamics of the computer forensics process would 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 must particularly name the place to be searched and the property to be seized, the Court has rejected the position that they must include “a specification of the precise manner in which they are to be executed.”¹⁶⁸ “On the contrary,” the 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 judicial review for reasonableness.¹⁶⁹ Judicial review occurs *ex post*, not *ex ante*.

In the last decade, however, a handful of courts and commentators have suggested that computer warrants merit a “special approach”¹⁷⁰ that requires the government to articulate *ex ante* the search strategy that forensic specialists must follow when searching computer hard drives.¹⁷¹ The thinking behind these proposals is that requiring a judge to preapprove specific steps will limit the scope of the search.¹⁷² The initial appeal is clear. If articulating a search protocol can limit the search that occurs, the resulting search is more likely to be narrow and particular. The *ex ante* strategy is deeply flawed, however. It wrongly assumes that prosecutors and magistrate judges have the knowledge needed to articulate search strategies before the search begins. In truth, the forensics process is too contingent and unpredictable for judges to establish effective *ex ante* rules. Legal regulation of computer searches therefore should be imposed *ex post*, not *ex ante*, just like regulation of physical searches.

1. *Computers and the “Special Approach.”* — The idea of articulating an *ex ante* search strategy is sometimes attributed to a 1982 Ninth Circuit case, *United States v. Tamura*.¹⁷³ In *Tamura*, the government seized boxes of documents and took them offsite for review. The boxes

¹⁶⁸ *Dalia v. United States*, 441 U.S. 238, 257 (1979). In *Dalia*, the government obtained a warrant to conduct electronic surveillance, which the police installed by covertly entering the place. *Id.* at 245. In an opinion by Justice Powell, the Court rejected the defendant’s contention that the warrant had to state *ex ante* that it permitted covert entry. *Id.* at 258–59.

¹⁶⁹ *Id.* at 257.

¹⁷⁰ *United States v. Carey*, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999).

¹⁷¹ See *supra* notes 134–145.

¹⁷² See *supra* notes 135–143.

¹⁷³ 694 F.2d 591 (9th Cir. 1982).

contained documents that were evidence of crime commingled with many other innocuous documents, and the government seized all of the boxes because it would have been infeasible to search through them at the site.¹⁷⁴ Judge Betty Fletcher's opinion approved the seizure but offered a "suggest[ion]" for how the government could "generally" avoid violating Fourth Amendment rights in cases involving commingled documents: get prior permission to seize all of the documents and conduct an offsite search, so that "wholesale removal" is "monitored by the judgment of a neutral, detached magistrate."¹⁷⁵ 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.¹⁷⁶

In an influential 1994 article, Raphael Winick took this idea and added an important twist.¹⁷⁷ Winick noted that computers used in criminal activity will contain a great deal of innocent material commingled with criminal evidence, and he urged courts to apply "the *Tamura* rule" to computers.¹⁷⁸ So far, so good. The rub is that Winick's vision of the *Tamura* rule was quite different from 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.¹⁷⁹ Winick proposed the "basic principle . . . that before a wide-ranging exploratory search is conducted, the magistrate should require the investigators to provide an outline of the methods that they will use to sort through the information."¹⁸⁰ Although framed as merely an application of *Tamura*, Winick's approach in fact urges a considerable shift in how courts regulate Fourth Amendment searches.¹⁸¹ The particularity requirement of the Warrant Clause requires the warrant to say *where* the search will occur, and for

¹⁷⁴ *Id.* at 595.

¹⁷⁵ *Id.* at 595–96.

¹⁷⁶ *Id.*

¹⁷⁷ Winick, *supra* note 1.

¹⁷⁸ *Id.* at 104–06.

¹⁷⁹ *See id.* at 107 ("A second warrant should be obtained when massive quantities of information are seized, in order to prevent a general rummaging and ensure that the search will extend to only relevant documents.").

¹⁸⁰ *Id.* at 108.

¹⁸¹ 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 approach is concerned with minimizing the intrusiveness of computer searches.

what, but courts have not interpreted it to require the warrant to specify *how* the police will execute the search.¹⁸²

Despite the questionable provenance of the Winick approach, the Tenth Circuit relied on it in important dicta in *United States v. Carey*.¹⁸³ In *Carey*, an officer searching a computer pursuant to a warrant for evidence relating to narcotics came across images of child pornography. He then abandoned the search for the evidence named in the warrant and began to look for additional images of child pornography.¹⁸⁴ The *Carey* court concluded that the search for additional images was improper,¹⁸⁵ citing Winick and *Tamura* in support of a “special approach”¹⁸⁶ to avoid discovering evidence outside the scope of the warrant in computer searches. The court advised: “Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, 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.”¹⁸⁷ The Tenth Circuit reemphasized the point a year later in a similar case, *United States v. Campos*.¹⁸⁸

Interest in including search protocols in warrants was heightened by the publication of the Justice Department’s 2001 manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.¹⁸⁹ The DOJ Manual suggested that it may be a “good practice” in some cases for affidavits to explain the techniques used to search a computer pursuant to a warrant.¹⁹⁰ The Manual further noted that “the Fourth Amendment does not generally require

¹⁸² See *Dalia v. United States*, 441 U.S. 238, 257 (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 . . .”).

¹⁸³ 172 F.3d 1268 (10th Cir. 1999).

¹⁸⁴ *Id.* at 1270–71.

¹⁸⁵ *Id.* at 1276.

¹⁸⁶ *Id.* at 1275 n.7.

¹⁸⁷ *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.”).

¹⁸⁸ 221 F.3d 1143, 1148 (10th Cir. 2000) (quoting *Carey*, 172 F.3d at 1275). In *Campos*, however, the court found that “the officers . . . did not expand the scope of their search in a manner not authorized by the warrant.” *Id.*

¹⁸⁹ DOJ MANUAL, *supra* note 1. In the interest 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.

¹⁹⁰ *Id.* at 96 (“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.”).

such an approach,” but pointed to *Carey* and *Campos* as signs that at least the Tenth Circuit preferred it.¹⁹¹

The combination of *Carey* and the DOJ Manual has led to a recent surge in 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 met mixed results, and outcomes appear to hinge in large part on each judge’s perception of how easy it is to search a computer hard drive for evidence. For example, in *United States v. Hill*,¹⁹² 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.¹⁹³ But judges with greater confidence in their ability to recognize and require proper *ex ante* restrictions on computer forensics analysis have reached different conclusions. For example, in one recent case, investigators had probable cause to believe that the defendant kept evidence of tax fraud on a computer stored in her apartment,¹⁹⁴ but a magistrate judge in Chicago refused to issue a warrant until the government provided a search protocol.¹⁹⁵ The court justified its decision on four grounds: first, computer searches 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 allows the government to conduct a highly targeted search if it chooses to do so.¹⁹⁶

2. *Rejecting Ex Ante Restrictions for Computer Warrants.* — With this history and doctrine in mind, we are now ready to answer the normative question: should courts adopt a search protocol requirement? The answer hinges on an important practical point: the computer forensics process is contingent, fact-bound, and quite unpredictable. Before an analyst starts searching a storage device, he normally has little idea which operating system the computer is running, what software is on it, how that software was used, what else is on the hard

¹⁹¹ *Id.* at 97.

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

¹⁹³ *Id.* at 1090–91.

¹⁹⁴ *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 955 (N.D. Ill. 2004).

¹⁹⁵ *Id.* at 962–63.

¹⁹⁶ *Id.* at 958–59; *see also* *United States v. Barbuto*, No. 2:00CR197K, 2001 WL 670930, at *5 (D. Utah Apr. 12, 2001) (suppressing evidence due to the absence of a search protocol). *But see* *United States v. Maali*, 346 F. Supp. 2d 1226, 1246 (M.D. Fla. 2004) (upholding the search despite a lack of search protocols, on the ground that “[w]hile it may be preferable and advisable to set forth a computer search strategy in a warrant affidavit, failure to do so does not render computer search provisions unduly broad”).

drive, or whether the suspect took steps to hide, misname, or otherwise disguise files. Perhaps the defendant made no effort to hide incriminating files; perhaps he changed file extensions, altered file headers, encrypted files, or took other steps to thwart the forensics process.¹⁹⁷

Nor will investigators necessarily know what forensic tool the analyst may use when performing his search. Different forensic tools have different features; 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 best suited 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*.

In light of these difficulties, magistrate judges are poorly equipped to evaluate whether a particular search protocol is the fastest and most targeted way of locating evidence stored on a hard drive. Given the contingent nature of the process, even a skilled forensic expert cannot predict exactly what techniques will 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. Although Winick and the *Carey* court are right that many techniques exist to target computer searches, they fail to realize that identifying the best technique usually must wait until the search occurs. Plus, warrant applications are *ex parte*; a judge must try to determine 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 officers need, 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. *Tamura* tried to ensure that a judge approved overbroad seizures before they occurred; the idea was that a judge could make the call whether an offsite search was necessary. 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 officers remove the property from the search location. Judges cannot

¹⁹⁷ See *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (noting that agents searching for computer files cannot be "required to accept as accurate any file name or suffix and limit [their] search accordingly" because criminals may "intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories").

exercise the same ex ante control over the forensics process, however. Analyzing a computer is a continuous process that involves performing hundreds or even thousands of individual steps. Judges cannot oversee them all. To do so competently, judges would need to stand alongside the forensic expert and approve each and every step as the situation evolved. The decision tree that an analyst might use to determine what steps to take is simply too long and complex for a judge to approve ex ante. To some extent, this dilemma parallels 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.¹⁹⁸ The computer forensics process calls for ex post standards, not ex ante rules.¹⁹⁹

D. Rethinking the Plain View Doctrine

If ex ante search protocols cannot effectively neutralize 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, and the particularity requirement no longer functions effectively as a check on dragnet searches. In this new environment, a tightening of the plain view doctrine may be necessary to ensure that computer warrants that are narrow in theory do not become broad in practice.

This section discusses three possible ways of narrowing 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 the exception based on the nature of

¹⁹⁸ See generally Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379 (1985) (discussing the rules versus standards dialectic in legal thought); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992) (analyzing the circumstances under which rules or standards are more desirable); Cass R. Sunstein, *Problems with Rules*, 83 CAL. L. REV. 953 (1995) (arguing the merits of both rule-bound and case-by-case decisionmaking).

¹⁹⁹ Search protocols may be useful in specific circumstances. For example, searches of computers believed to contain privileged documents present special concerns. In such cases, investigators may specify a search protocol to explain how the analysts will handle privileged documents. See, e.g., *United States v. Hunter*, 13 F. Supp. 2d 574, 578 (D. Vt. 1998) (describing the government's search protocol to avoid observing privileged files); *United States v. Neill*, 952 F. Supp. 834, 837 (D.D.C. 1997) (same). Similarly, searches of third-party computers, such as large computer servers, raise unusual problems. See, e.g., *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432, 440-41, 443 (W.D. Tex. 1993) (holding the Secret Service liable under the Stored Communications Act for seizing computer servers and taking them offsite despite a valid warrant). 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. This practice is now common in light of *Steve Jackson Games*. Investigators can give the search protocol to the server owner onsite to assure him that the search will be narrow. In general, however, review of search strategies should occur ex post, not ex ante.

the evidence discovered, permitting the use of some kinds of evidence while blocking others. Both of these proposals seem promising at first, but prove difficult to apply in practice. The third proposal is more draconian: it would abolish the plain view exception in digital evidence cases. Such a 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 could not be used against the defendant absent an application of the inevitable discovery doctrine. Eliminating the plain view exception for digital searches is not an ideal solution, and it may not be necessary today. But it may eventually prove the best way to restore the function of the Fourth Amendment in a world of digital evidence.²⁰⁰

1. *Approaches That Focus on the Circumstances of the Search.* —

One approach to narrowing the traditional plain view exception would factor in the circumstances of the search. For example, one method would involve overturning *Horton* and restoring the inadvertence requirement, placing the emphasis on the analyst's subjective intent. Another method would entail regulating the particular tools used during the forensic search; for instance, this approach might require the police to use particularly advanced forensic tools. Yet another method would permit plain view evidence when the specific forensic step that uncovered it 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 in the context of computer searches so that it focuses on the analyst's subjective intent. In *Carey* and *United States v. Gray*,²⁰¹ 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 for child pornography;²⁰² in *Gray*, the analyst continued to look for evidence of computer hacking but in doing

²⁰⁰ For the purposes of this discussion, I assume that courts take a somewhat holistic view of the role of the plain view exception 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 v. California*, 496 U.S. 128, 134 (1990) ("If 'plain view' justifies an exception from an otherwise applicable warrant requirement . . . it must be an exception that is addressed to the concerns that are implicated by seizures rather than by searches."). Under *Hicks*, however, obtaining copies of computer files does not constitute a seizure. 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. Although this proposition seems 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 this point. For my purposes, I will assume this existing judicial practice continues. To the extent that courts do recognize this technical point, its acknowledgement seems only to argue more strongly for doctrinal reform.

²⁰¹ 78 F. Supp. 2d 524.

²⁰² See *United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999).

so discovered more child pornography.²⁰³ In both cases, the courts focused on the subjective intent of the officer to either stay within or look beyond the scope of the warrant. When the officer looked for evidence described in the warrant, the discovered images could be used in court;²⁰⁴ when the officer looked beyond the warrant, the images were suppressed.²⁰⁵

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 positioned to answer (witness credibility). Judges are familiar with physical 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 complex and fluid. In this environment, a subjective test may serve as a second-best proxy for the objective test. Although judges may be poorly equipped to assess whether in fact an analyst's steps were consistent with a targeted search, they are better able to tell whether the analyst was at least *attempting* to conduct a good faith targeted search.

However, the subjective approach has a critical weakness. An officer's subjective intent may be difficult to discern. Proving intent 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.²⁰⁶ Such a policy can create General Tool through practice instead of technology. When every step taken by an analyst is a matter of routine policy, it becomes difficult to exclude evidence on the ground that the analyst was attempting to circumvent the warrant. Reliance on agency policy may explain *Gray*, in which 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.²⁰⁷ The existence of other-

²⁰³ See *Gray*, 78 F. Supp. 2d at 527.

²⁰⁴ See *id.* at 530 (permitting the use of files when the law enforcement agent "never abandoned his original search").

²⁰⁵ See *Carey*, 172 F.3d at 1276.

²⁰⁶ Interview with Mark Pollitt, *supra* note 39.

²⁰⁷ *Gray*, 78 F. Supp. 2d at 526–27.

wise laudable standardized practices makes the subjective intent approach much less helpful in practice than it first seems in theory.

Another 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 a judicially manageable standard. Dozens of different forensic programs exist, each with its own strengths, weaknesses, availability, and cost. The tools morph quickly over time, as do the latest techniques in hiding data. Which tool would be the best in any situation depends on how the officer was trained, how the tool was used, what techniques might have been 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 require use of particular tools at any particular time.²⁰⁸ 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-handed will never know whether General Tool might have uncovered something Perfect Tool did not. Given these competing considerations and difficult choices involving 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 extent of the privacy violation, and the relevant legal authority.²⁰⁹ Under this approach, plain view evidence discovered during reasonable searches would be admitted, while such evidence discovered during unreasonable searches would be suppressed. Such a case-by-case approach is an interesting option, but it may be difficult for courts to apply. First, for reasons explored earlier, it may be difficult for courts to identify exactly when a particular step is reasonable or unreasonable.²¹⁰ 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.²¹¹ For example, imagine that an analyst performs an examination in 100 steps, and that step 100 produces evidence of a crime beyond the scope of the original war-

²⁰⁸ 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.”).

²⁰⁹ 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 seizure and the government's legitimate needs).

²¹⁰ See *supra* pp. 575–76.

²¹¹ See *Wong Sun v. United States*, 371 U.S. 471, 484–88 (1963) (discussing the fruit of the poisonous tree doctrine).

rant. Assume that step 100 is constitutionally reasonable in isolation, but that steps 98, 95, 74, and 51 are not. To determine whether this evidence was admissible, the court would presumably need to find out the causal relationship between the earlier steps and step 100 to determine if the fruits of the latter are fruits of the poisonous tree. When such questions arise in the case of physical searches, judges better understand the causal relationships of physical searches. The computer forensics 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 in the context of digital searches.

2. *Approaches That Focus on Future Uses of 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 only for serious crimes, or only for terrorist offenses, but not allow evidence to be used for low-level offenses. Professor William Stuntz makes a suggestion along these lines in a recent essay.²¹² Professor 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 “limit the range of crimes the government can prove by evidence discovered through that tactic.”²¹³ Applied to the computer forensics process, the rule might be that the government could use evidence discovered in plain view only in specific types of prosecutions. Perhaps they could 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.²¹⁴

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 to prosecute terrorism. 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

²¹² William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2184–85 (2002).

²¹³ *Id.* at 2184.

²¹⁴ *See id.*

of criminal offenses that may be used in terrorism-related cases.²¹⁵ Is any case that involves any one of these crimes a terrorism case? Can any evidence of any of these crimes justify the introduction of plain view evidence, even if it is not particularly probative? Given that some of these statutes are worded quite broadly, can the government 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 alleged conduct does not seem to be primarily terrorism-related?

Second, any rule that hinges governmental power on the type of offense creates a strong incentive for Congress to expand the list of eligible offenses 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,²¹⁶ 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.²¹⁷ The list of eligible crimes was short in 1968, when the Wiretap Act was passed.²¹⁸ Over time the list has expanded considerably,²¹⁹ and now includes essentially every federal felony offense that is prosecuted with any regularity.²²⁰ Why? Because there are always going to be some instances 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 list to include that crime.

Finally, settling on a list of specific crimes that should qualify to admit 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 prime candidates for the list of offenses that allow the introduction of plain view evidence. On the other hand, the link between possession and actual molestation is presently unclear. Further, child pornography offenses are the most commonly prosecuted type of digital evidence crimes; given the current state of law and technology,

²¹⁵ See, e.g., 18 U.S.C.A. § 832 (Supp. 2005); 18 U.S.C.A. § 1993 (2000 & Supp. 2005), amended by Safe, Accountable, Flexible, Efficient Transportation Equity Act, Pub. L. No. 109-59, § 3042, 119 Stat. 1144, 1639-40 (2005); cf. 18 U.S.C. § 2331 (2001 & Supp. II 2002).

²¹⁶ 18 U.S.C.A. §§ 2510-2522 (West 2000 & Supp. 2005).

²¹⁷ *Id.* § 2516(1).

²¹⁸ See JEFFREY ROSEN, *THE UNWANTED GAZE* 37 (2001).

²¹⁹ See *id.*

²²⁰ See 18 U.S.C.A. § 2516(1)(a)-(r).

concerns about pretextual searches may be most justified in the case of a government agent obtaining a warrant for a low-level crime to see if he can find any child pornography on a suspect's computer. The right balance to strike isn't clear; over time it may change, and there may be a different answers for different types of offenses. Courts seem poorly suited to draw such lines,²²¹ and legislative line-drawing seems likely to result in a broadening over time. Although these objections do not rule out such a tailored approach, they provide reason to view it with considerable caution.²²²

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 inevitable discovery doctrine removed the taint.²²³ This approach would permit forensic investigators to conduct whatever searches they deemed necessary, and to use General Tool or its equivalent however they liked, with the caveat that only evidence within the

²²¹ See Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 857–87 (2004).

²²² In a thoughtful student note, David Ziff argues that the fact that the incriminating nature of discovered evidence must be “immediately apparent” to fall within the plain view exception should act as a natural limit on the plain view doctrine in computer searches. See David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 869 (2005). The incriminating nature of image files such as those containing child pornography is immediately apparent; the incriminating nature of text-based files such as letters 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 a number of courts have construed the “immediately apparent” requirement less strictly than Ziff's analysis expects. These courts have admitted documentary evidence under the plain view exception even when discovery of the incriminating nature of the documents required considerable analysis. See, e.g., *United States v. Khabeer*, 410 F.3d 477, 482 (8th Cir. 2005) (admitting under the plain view exception receipts and identity documents beyond the scope of the warrant in a fraud case); *United States v. Calle*, No. 98-50377, 1999 WL 313361, at *1 (9th Cir. Mar. 22, 1999) (holding travel documents admissible under the plain view exception because the officer read the documents and saw that the dates on them were inconsistent with defendant's statements to officer); *United States v. Calloway*, 116 F.3d 1129, 1133 (6th Cir. 1997) (holding notes, bank receipts, and power of attorney found during search for other types of documents evidencing aircraft piracy admissible under plain view exception). A second difficulty with Ziff's argument is that computer searches generally occur offsite through repeated searches on the government's imaged copy, rather than onsite 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 viewing of the data, or also to subsequent viewings. If the former, it may be difficult to distinguish initial viewings from subsequent viewings. If the latter, officers will have repeated opportunities for the incriminating nature of the evidence to become apparent.

²²³ See generally cases cited *infra* note 227.

scope of the warrant normally could be used in court. Dragnet searches would be neutralized by a rule ensuring that only evidence within the scope of proper authority could be used. Statutory privacy rules resembling the nondisclosure rule for grand jury testimony would presumably be needed to supplement this protection;²²⁴ such rules could ensure that evidence beyond the scope of a warrant was not only never used in court, but also never disclosed.²²⁵

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, and a decade from now, it will probably seem obviously flawed. The need for new rules is emerging, but eliminating the plain view exception would be too severe at present. As time passes, however, that will likely change. Abolishing the plain view exception may 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 balance the competing needs of privacy and law enforcement in light of developments in computer technology and the digital forensics process.²²⁶ Forensic analysis is an art, not a science; the process is contingent, technical, and difficult to reduce to rules. Eliminating the plain view exception in digital evidence cases 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. At the same time, the approach would protect 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 it may be the best available rule. Although forensic practices may be invasive by technological necessity, a total suppression rule for evidence beyond the scope of a warrant would both remove any incentive for broad searches and neutralize the effect of broad searches that occur. It would regulate invasive practices by imposing use restrictions *ex post* rather than attempting to control searches *ex ante*, offering a long-term second-best approach to

²²⁴ See generally FED. R. CRIM. P. 6(e).

²²⁵ Cf. Stuntz, *supra* note 212, at 2183–84 (considering a rule that would permit evidence discovered during broadly permitted searches to be revealed only through criminal trials).

²²⁶ Cf. Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 75 (1995) (suggesting that “use restrictions” on evidence obtained through government searching in general may “accommodate the government’s interest in obtaining information with individuals’ interest in confining disclosure of private information as much as possible”).

regulating the computer forensics process. In short, it would allow the police to conduct whatever search they needed to conduct (to ensure recovery) and then limit use of the evidence found (to deter abuses).

Notably, eliminating the plain view exception would not mean that all evidence beyond the scope of a warrant need be excluded from use for all time. For one thing, the independent source and inevitable discovery rules would still apply. Under these closely related doctrines, evidence can be 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.²²⁷ Application of these doctrines in the computer search context can 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 search a computer for tax fraud and then come across child pornography, whether the police are able to use the child pornography in a separate prosecution would hinge on whether they can show that they would have come across the evidence absent the initial fraud investigation.

CONCLUSION

The new dynamics of computer searches and seizures 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 containers. The mechanisms of home and container searches directed Fourth Amendment doctrine to focus primarily on the entrance to the home or container. In a world of physical barriers, actions that broke down those physical barriers became the focus of judicial attention. The world of digital search and seizure shows that this focus is contingent on the architecture of physical searches. As computer searches and seizures become more common in the future, we will begin to see twentieth-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 attempts 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 I recommend share a number of common themes with the physical rules. The exposure-based approach to digital searches offers a vir-

²²⁷ See *Murray v. United States*, 487 U.S. 533, 536-41 (1988) (explaining the independent source doctrine); *Nix v. Williams*, 467 U.S. 431, 440-48 (1984) (discussing the inevitable discovery exception to the exclusionary rule).

tual 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 proper 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*²²⁸ 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 perhaps 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 a vital 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 how to regulate government access to information. The dynamics of criminal investigations in physical space support one set of answers to this question. The dynamics of investigations involving digital evidence may support another.

²²⁸ 389 U.S. 347 (1967).